Human Risk Contributions in Process Industry: Guides for Their Pre- Identification in Well-Structures Activities and for Post-Incident Analysis

Pedersen, Ole Michael Kristian

Publication date:
1985

Document Version
Publisher's PDF, also known as Version of record

Risø-M-2513

RISØ

Risø-M-2513

Human Risk Contributions in Process Industry: Guides for Their Pre-Identification in Well-Structured Activities and for Post-Incident Analysis

O. M. Pedersen

Risø National Laboratory, DK-4000 Roskilde, Denmark
May 1985

RISØ-M-2513

HUMAN RISK CONTRIBUTIONS IN PROCESS INDUSTRY: GUIDES FOR THEIR PRE-IDENTIFICATION IN WELL-STRUCTURED ACTIVITIES AND FOR POST-INCIDENT ANALYSIS

O. M. Pedersen

Abstract. The report should be considered a guide for the treating of human errors: for identifying their possibilities of occurrence when designing well-structured human tasks and for their improvement when they occur in reality.
For these purposes a strong coupling between predictive and retrospective analysis is emphasized: In order to control human errors, post-incident analysis of cases with human errors in a given industrial plant should be performed as means of feedback from reality for the verification of results of predictive analysis and also as a general means of identifying and improving such human errors which cannot be expected covered by predictive analysis.

cont.

May 1985
Risø National Laboratory, DK-4000 Roskilde, Denmark

Primarily, the guide addresses people with a knowledge of the technical plant in question and involved in the safety-oriented design and improvement of human activities and without a particular human factors background.

The main report describes the procedures for post-incident analysis and for Work Analysis, which is a search strategy developed for well-defined activities, e.g. test and calibration, and constitutes a formalized procedure for the pre-identification of relevant human errors leading to a lack of task result and/or to immediate effects not covered by the lack of task result itself.

Work Analysis and the post-incident analysis procedure are based on a common description system for human malfunctions. This system is explained in appendix and so are its underlying models and way of reasoning.

Finally, a word index is provided for supporting the reader.

4 references. In English.

ISBN 87-550-1124-1
ISSN 0418-6435

Grafisk Service Center 1985

CONTENTS

PREFACE

This report is one of a series belonging to that part of the LIT-1 project concerned with defining, developing, evaluating and disseminating a methodology for the identification of human malfunctions in test and calibration.
In previous reports requirements to and proposals for search strategies were given (NKA/LIT-1(82)101, Risø-M-2351) and incidents reported from nuclear power plants were studied to get indications of how different types of human error could be covered by analytical prediction or by risk management, respectively (NKA/LIT-1(84)107, Risø-M-2470). One strategy: Work Analysis, was proposed and subjected to a trial application (NKA/LIT-1(84)408, Studsvik Technical Report NR-85/26).
In the present report (NKA/LIT-1(84)106, Risø-M-2513) a guide is provided for the predictive method: Work Analysis, and for post-incident analysis of human malfunctions. A rather detailed level has been found necessary in order to serve practical applications: Human malfunctions, generally, are determined by details and this necessarily will be reflected in a guide for their treatment.
The work was financed partially by the Nordic Board of Ministers and the Swedish Nuclear Power Inspectorate (SKI).

EXECUTIVE SUMMARY

Primarily, the guide addresses people with a knowledge of the technical plant in question and involved in the safety-oriented design and improvement of human activities and without a particular human factors background. Also the guide addresses people involved in probabilistic risk analysis and risk management.

In principle, two main possibilities exist of coping with human as well as other kinds of risk contributions:

1) their pre-identification and elimination, as far as possible, during the design of a human task and in a pre-construction risk analysis,

2) to improve or counteract them when they occur in practice.

The two problems should be considered in coherence and by so doing, the following concept has been arrived at: The information provided by performing a Probabilistic Risk Assessment (PRA) or an As-operated Safety Analysis Report (ASAR) should be used as reference for a closed-loop risk control or Risk Management (RM) utilizing post-incident analysis as means of feedback of operational experience, this is named "the PRA/RM concept".

The search method "Work Analysis" (WA) and the post-incident analysis procedure are intended for fitting into the PRA/RM concept and for satisfying its documentation requirements, thus offering a unified approach for the treating of risk-related human activities in their design and improvement and in monitoring malfunctions in their performance:

Work Analysis is developed for well-defined activities, e.g. test and calibration, and is a formalized procedure for the pre-identification of relevant human errors leading to a lack of task result and/or to immediate effects not covered by the lack of task result itself. The method makes possible a systematic documentation of risk-related intentions of / reasons for the task design and/or its modifications.

The problems of quantified assessment of human reliability and risk contribution are not discussed: For the WA procedure the steps where quantification may be attempted are mentioned and some concise criteria for quantification are quoted.

The post-incident analysis procedure will provide a systematic human-oriented description and documentation of incidents involving human malfunctions, also in activities not covered by PRA and, therefore, to be controlled by RM. Thus, the post-incident analysis makes possible the systematic feedback for monitoring the quality of task performance.

WA and the post-incident analysis procedure are based on a common description system. This system is explained and so are its underlying models and way of reasoning. The important properties of the description system are that it enables the analyst

- in post-incident analysis to identify a causally ordered chain of descriptors connecting an external cause of the human malfunction with an external manifestation of the effect of the malfunction through two human-oriented descriptors of a general, not task-specific, kind,
- in predictive analysis to postulate relevant causally-ordered chains of the same kind as above and to generate relevant scenaria.
- to have the chain of descriptors connected with a conventional task description given in equipment-oriented terms.

Only the main principles for incorporation of the WA into an overall plant PRA are described as guided by the PRA/RM concept, a detailed treatment will be dependent on actual circumstances for PRA and RM. However, one could expect in relation to a PRA or an ASAR more complete identification, description and documentation of relevant event sequences related to human activities by using the WA method as a predictive tool and the post-incident analysis as a means of feedback of operational experience.

In a long-time perspective it could be expected to have provided from post-incident analyses a systematic collection and classification of information on human performance including quantified data for improving the quantified assessment of human risk contributions, if such improvement is needed and collection of information is feasible.

1. INTRODUCTION

Two main possibilities exist of coping with human risk contributions:

1) their pre-identification and elimination, as far as possible, during the design of a human task and in a pre-construction risk analysis,

2) to improve or counteract them when they occur in practice.

The two problems should be considered in coherence and by so doing, the following concept has been arrived at: The information provided by performing a Probabilistic Risk Assessment (PRA) or an As-operated Safety Analysis Report (ASAR) should be used as reference for a closed-loop risk control or Risk Management (RM) utilizing post-incident analysis as means of feedback of operational experience, see Figure 1.1. In the following, this will be referred to as "the PRA/RM concept". For this concept to operate in practice, the requirements given in Figure 1.1 should be fulfilled. For a comprehensive discussion the reader is referred to ref. 1.

The search method "Work Analysis" (WA) and the post-incident analysis procedure are intended for fitting into the PRA/RM concept and for satisfying its documentation requirements. They are based on a common system for the description of human malfunctions as presented in detail in Appendix A.

Section 2 describes a post-incident analysis procedure for incidents with human malfunctions. In addition to the human malfunction descriptors a set of description elements is applied for the overall description of an incident in order to ensure some uniformity and compatibility when characterizing different incidents. Relations between post-incident analysis, PRA and RM are described at the end of the section.

Section 3 firstly relates the Work Analysis method with different task types, their analyzability and treatment for the control of risk. An overview of the method is given, followed by the detailed formalized procedure and the incorporation of

the method in a PRA is briefly outlined.
Finally, the problems related with quantification of human risk contributions are summarized by quoting some previously stated criteria for meaningful quantification. The WA method and, particularly, the description system for human malfunctions should be considered basic qualitative steps towards more meaningful quantification.

The index is composed with the particular intent of supporting the reader in acquiring familiarity with terms, definitions, etc.

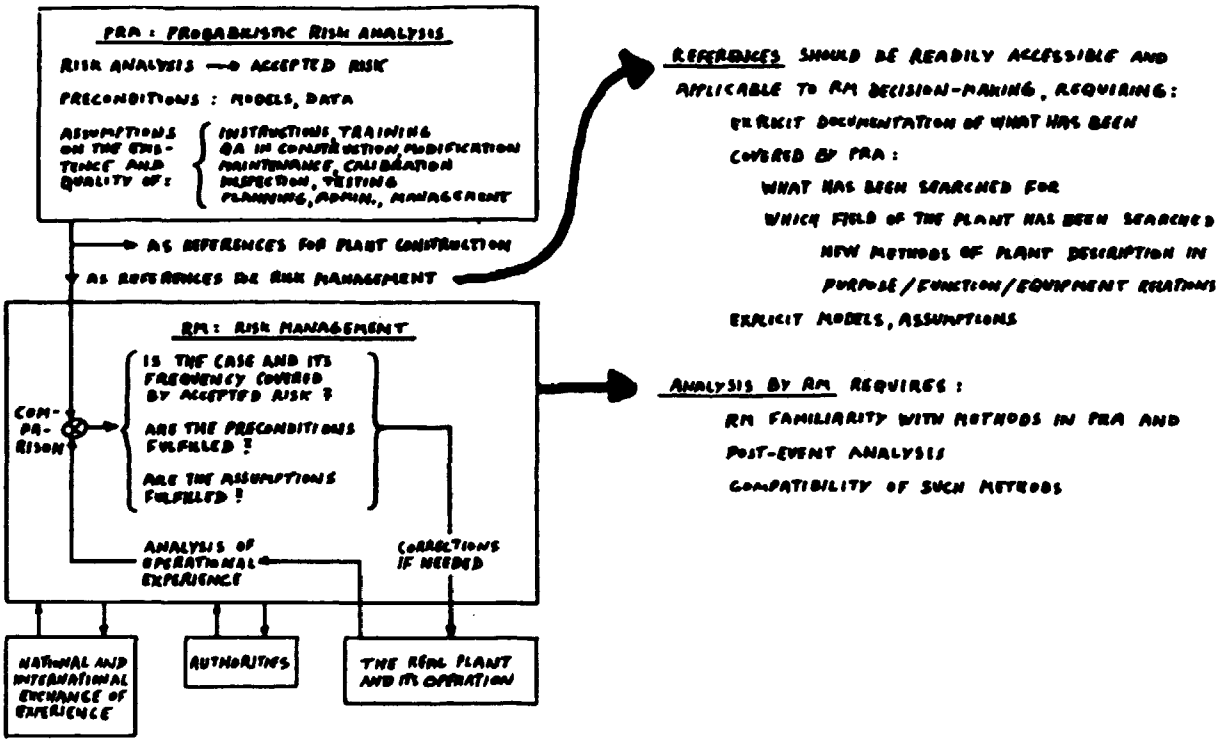


Figure 1.1: The information provided by performing a probabilistic Risk Assessment should be used as reference for a closed-loop risk control or Risk Management utilizing post-incident analysis as means of feed-back of operational experience.

2. POST-INCIDENT ANALYSIS

Emphasis should be given to the procuring of an easily accessible, condensed, unambiguous verbal description of the incident, particularly of the human involvement, these properties being conserved in re-use of the description at later occasions.

If systematic collection of information from many incidents is planned, the descriptors to be used should be selected with care for the sake of unambiguous coverage for the intended use of such a data collection system. In ref. 3 requirements for such a system are discussed and examples of descriptor categories are presented.

Clarification of human involvement in incidents is rendered increasingly difficult as a function of time elapsed after their occurrence. The human-oriented categories described in Appendix A should promote such clarification in a systematic and impartial manner, e.g. by identifying lacking information and planning questions for the impartial procuring of such information, ending up with an incident description where the causal flow and the mechanisms controlling the event propagation are maintained and can be regenerated from the description.

Even analyses of single, simple cases are worthwhile as they can help identify important typical ingredients of more severe incidents.

In the following discussion, the reader is supposed to be familiar with the way of reasoning presented in Appendix A about the background and use of the description system and its models.

In order to secure consistent treatment of human malfunctions relative to the total sequence of events involved in an incident, it is practical to have some uniformity in the description of the incident in total. Fig. 2.1 gives the

elements of such a description: In the following subsections we move from the focal point: the human error and its cause, to the activities, in which errors occurred, and finally to the event sequence subsequent to the error.

2.1. The Error and Its Cause

Errors, to be distinguished from technical failures, are used for human malfunctions without taking an attitude towards guilt, responsibility, misleading from erroneous instructions etc.

Errors are found by the search for causes: Pragmatic stop-rules for the search could be to stop at a point in the causal sequence which can be accepted as an explanation of where, if needed, efficient means of improvement can be implemented.

An error can be characterized in human-oriented terms by the categories: Internal human malfunction and psychological error mechanisms, of the description system in Appendix A.

The categories are described in detail in Appendix A and flow-graph guides for their use are given in Figures 2.4 and 2.5 for internal malfunction and mechanisms, respectively.

Causes of errors: directly causally coupled with and previous to an error.

A cause can be characterized by the category: External cause of malfunction, in the description system. The connection with the human-oriented categories: "Psychological mechanisms" and "internal malfunctions" is described in Appendix A. A flow-graph guide for using the category: external causes, is given in Fig. 2.3.

Human factors-oriented influences with the potential of promoting the error, however, not being direct causes, can be described by the categories: Situation factors and Factors shaping performance, in the description system. Flow-graph guides for the use of parts of these categories are given in Figures 2.6 and 2.7.

Conditions: Circumstances external to the erroneous activity, in plant-oriented terms and influencing the error, however, not to be considered causes as defined above. Could be stated in terms such as the descriptors 10-20 in Fig. 2.1.

Relations between errors and between errors and their causes give rise, during the incident analysis, to questions such as

- Was the error caused/influenced by previous errors or by circumstances/conditions?
- Was, for the same person, one error leading to subsequent errors?
- Was the error owing to a well-meant, however, due to circumstances inappropriate intention?

2.2. Erroneous Human Activities

An erroneous activity may directly affect the technical plant or may belong to previous phases, e.g. planning or making instructions.

As an example, in Fig. 2.2 are shown activities generally related with a test or calibration task. The task directly affecting the plant is the box in the center of the figure.

The activities directly in touch with the plant are in general much formalized, i.e. determined by instructions and procedures. This is possible because the well-defined structure of technical systems can be reflected in instructions for their handling, the purpose of the instructions is to ensure reliable handling.

The degree of formalization is decreased when we move away from these activities, e.g. into phases of planning, design and administration of the task in question, these consequently being less accessible for the identification of causal sequences in post-incident analysis. However, if improvements are found necessary, it is important to identify and distinguish between activities that are well-structured and hence can be "designed for reliability", and other activities, which have to be kept reliable by administrative precautions, see subsection 2.4.

A description should be given of the activity directly influencing plant technical systems and plant physical parts and during which the error manifested itself as an abnormal influence on the plant.

Also the activity during which the error was committed should be described if this activity is different from that above.

Further, activities or events intervening the above two types of activities may be of interest if studying possibilities for improvements, particularly "error recovery points".

The descriptors L1-L13 for task category in Fig. 2.1 should be considered examples.

Task disturbances: The incident analysis should identify whether the error occurred during improvisation due to disturbance of an otherwise well-defined task. The descriptors 21-24 in Fig. 2.1 for the source of disturbance could be applied.

2.3. The Effects of Error

In this paragraph the following terms from Fig. 2.1 are defined:

The error effect
- loss of task result
- immediate effect
- coupling between lost result and immediate effect
- error effect owing to combination of error and condition
- multi-effect, potential for multi-effect

The ultimate effect
- ultimate effect owing to combination of error effect and condition.

For providing a condensed description of the total event sequence subsequent to the error, as a minimum it should be mentioned whether the error effect is owing to a combination of the error and other independent circumstances and similarly for the ultimate effect: whether it was owing to a combination of the error effect and other independent circumstances.

An incident could appear as being of minor importance judging from its ultimate effect or from combinatorial effects not likely to be repeated: Still it is considered important to evaluate each element of the event sequence in isolation as an indicator of possible weaknesses to be improved. Also dependences and couplings between elements should be considered.

Effect of error = the manifestation of the abnormal influence of the error
- on the physical plant
- found when causally backtracking
- causally near to task

The effect can be described in terms of category: External human malfunction, in the description system of Appendix A.

The effect can be
- the consequence of a human activity/task in isolation, i.e. without task-external causes or conditions,
- the combinatorial effect of a human activity and a task-external condition, these in combination leading to the effect. For task-external conditions, the descriptors 10-20 in Fig. 2.1 can be considered plant-related examples.

The effect can be:
- Lack of the specified task result (Reliability analysis, as part of WA, is concerned with errors leading to this type of effect as described in section 3).
- An immediate effect = an effect contributing to risk in a way not related to the lack of task result, but to the specific causal effect of an erroneous act during the task/activity. (Search for immediate effects, as part of WA, is concerned with errors leading to this type of effect as described in section 3). The immediate effect can influence a system or component related or not related to the task.

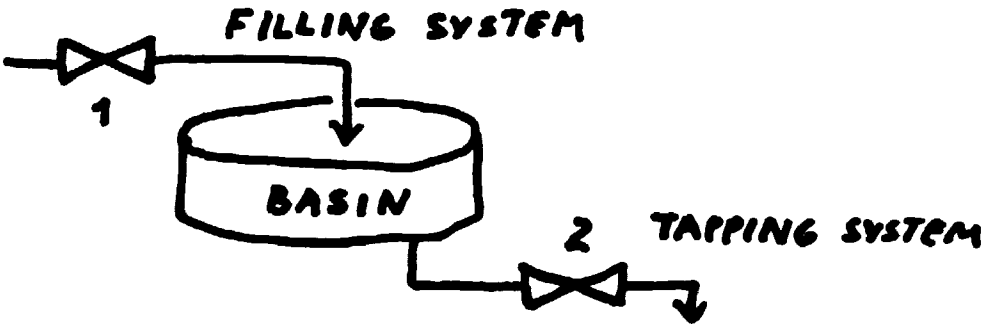
  Example 1: During a task a valve should be brought from open to closed position. By mistake a different valve belonging to an unrelated system is closed instead: lack of task result and immediate effect in unrelated system. Often in this type of event

the immediate effect only is significant for the event.

Example 2: Error in calibration task leading to wrong calibration: Task result lacking (usually not of importance for the event because the old calibration state would probably be satisfactory) and immediate effect (= the inappropriate new calibration state of instruments, possibly with less margin to safety).

Coupling between lack of task result and immediate effect can lead to particular effects as examplified in the following:

Example 3:



Task in filling system: Closing of valve 1.
Error: valve 2 is mistaken for valve 1 and 2 is closed.
Lack of task result: valve 1 is not closed.
Immediate effect in different system: Tapping system closed. Basin overflow, due to combination of lack of task result and immediate effect.

Example 4: During a task a valve should be brought from open to closed position. By mistake the valve is left half open this leading to an effect on the system involved in the task, an effect not covered by the specification of the task result: lack of task result and an immediate effect related to the task.

Multi-effect: If the activity, during which the error effect manifested itself, was repeated on several physical parts of the plant, we have a multi-effect. Also it should be mentioned explicitly if a case is judged to have significant potential for leading to multi-effect.

Ultimate effect describes the end of the event sequence, e.g. in terms of descriptors 1-3 in Fig. 2.1.

2.4. Post-Incident Analysis: Its Relationship with PRA and RM

According to the PRA/RM concept mentioned in section 1 the risk imposed by an industrial process plant, for instance nuclear power plant, is controlled in two ways: Firstly, by a plant construction based on a PRA. Secondly, by RM, i.e. administration of the results and preconditions of the PRA which act as requirements for plant construction and operation. In addition, through the plant lifetime, the results and preconditions of the PRA serve as references for inspections, tests and analyses of operational experience: By post-incident analyses operational experience is compared systematically with the reference information provided by the PRA in order to support RM decisions serving to maintain the designers' safety design targets and to reveal oversights and design errors. For a discussion of this and the consequent requirements to the analytical methods see ref. 1.

In accordance with the above PRA/RM concept the following can be stated as the main purposes of post-incident analysis, particularly for human activities and their risk contributions:

- To identify and distinguish between: errors in well-structured activities which have been considered in the plant PRA and, therefore, are included in the accepted risk (only the frequency of such errors should be supervised), and: errors which are not included in the PRA and therefore have to be counteracted by administrative precautions.
- To ensure that the PRA or ASAR for the plant is updated or supplemented by the identification, description and docu-

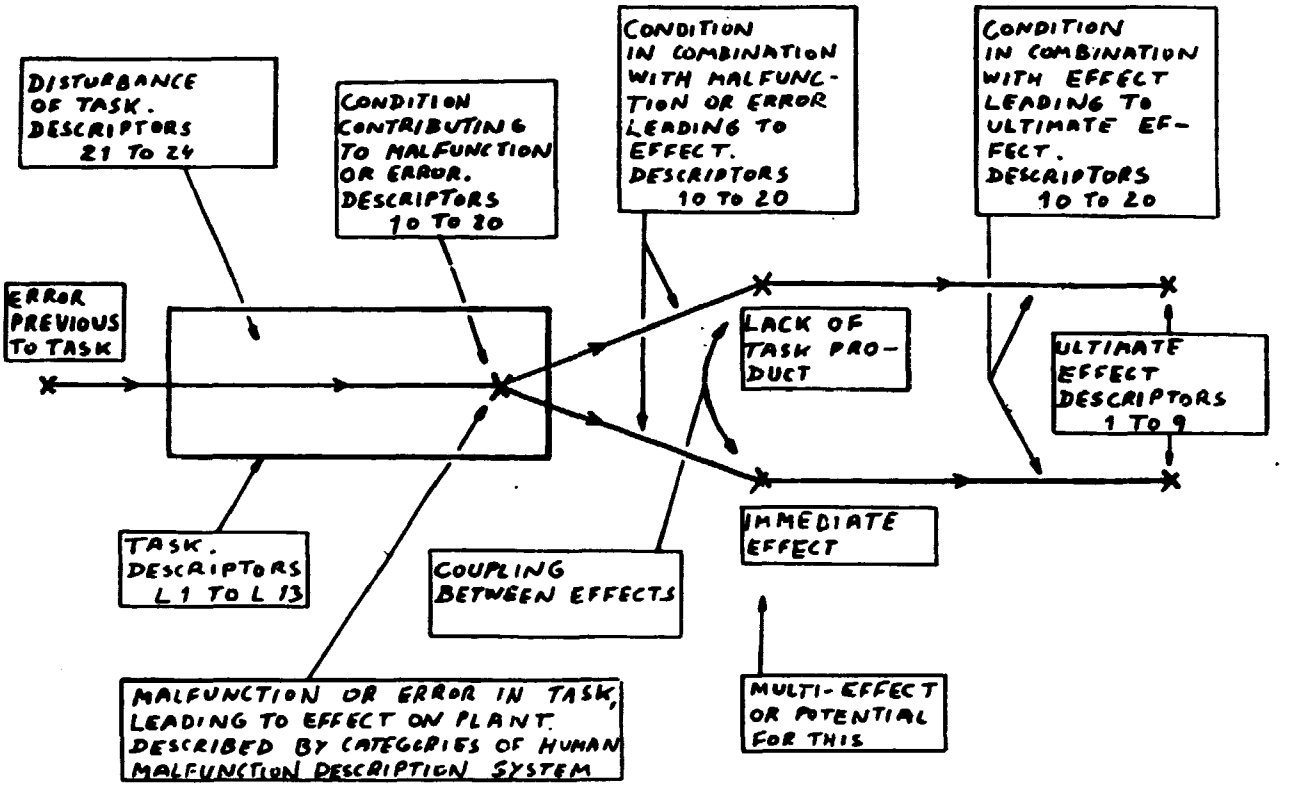
mentation of significant event sequences not covered by the PRA/ASAR, particularly those involving human malfunctions.

How the above purposes could be fulfilled in practice depends on circumstances determined by the actual plant PRA/ASAR and RM and is outside the scope of the present guide. However, at a rather general level questions of the following kinds could be asked during the analysis:

Are the elements of the incident expected occurrences within the boundaries of the PRA or outside the boundaries, needing initiatives for improving system, operational practice or risk analysis?

How could elements of the incident influence risk, e.g. in the following ways:

- by contributing insignificant increase in a failure frequency already covered by postulated random component failures
- by contributing significant increase in frequency of accidental event chain including break of recovery path
- by having the potential for contributing causal coupling between events otherwise considered independent in the PRA.



LIST OF EXAMPLE DESCRIPTORS

Task Category

- L1 Design and design changes of equipment
- L2 Tools and procedure design and modification
- L3 Fabrication
- L4 Installation
- L5 Inspection
- L6 Operation
  - L6.1 Monitoring: General information sampling and judgement to monitor overall system state
  - L6.A Supervisory process control: Act as supervisor/adviser for other operator or perform autocontrol of L6.A, L6.B or L6.C
  - L6.A Configuration control in order to change process function, e.g. valve line-up, switching including auto/manual
  - L6.B Check and verification of system configuration
  - L6.C Change of operational state e.g. start, stop
  - L6.D Coordination of state, e.g. match state to reference or other system
  - L6.E Other or not specified
- L7 Test and calibration:
  - L7.1 Getting access to location for work (including getting permit)
  - L7.2 Preparation of equipment and tools
  - L7.3 Execution of the actual test and calibration activity
  - L7.4 Restoration, removal of tools etc.
- L8 Maintenance and repair (modification etc.):
  - L8.1 Getting access to location for work (including getting permit)
  - L8.2 Preparation of equipment and tools
  - L8.3 Execution of the actual maintenance activity
  - L8.4 Restoration, removal of tools etc.
- L9 Logistics
- L10 Administration: recording, reporting, planning etc.
- L11 Management: resource allocation and supervision
- L12 Other not covered above
- L13 Not stated, not applicable

1 - normal operation
2 - protective function
3 - barrier (including b. incapacitated, release through b.)

4 The ultimate effect of the event is judged to be an expected occurrence within the boundaries of risk analysis.

5 The ultimate effect of the event is judged to be outside the boundaries of risk analysis
6 - shift supervisor (minor variability, cases related to individual persons etc.).
7 - plant operations management (work planning, local conditions peculiar to plant).
8 - utility level (design, PRA deficiencies, major risk and reliability issues).
9 - authorities (as utility level and in addition: risk to environments).

10 - oversight in plant design
11 - unknown property of technical equipment
12 - oversight in, inadequate model used for RA
13 - oversight in construction manufacturing phase of plant degradation in
14 - plant technical system
15 - use of procedures
16 - design or updating of procedures
17 - maintenance, test, calibration, modification, repair, inspection
18 - training, education
19 - work planning, scheduling, administration, management
20 - other not covered above

21 - failure, abnormal state of technical system
22 - lack of tools, equipment
23 - lack of material, spare parts
24 - other task, order, difficult access etc.

Figure 2.1: Formal event description, its elements and example descriptors.

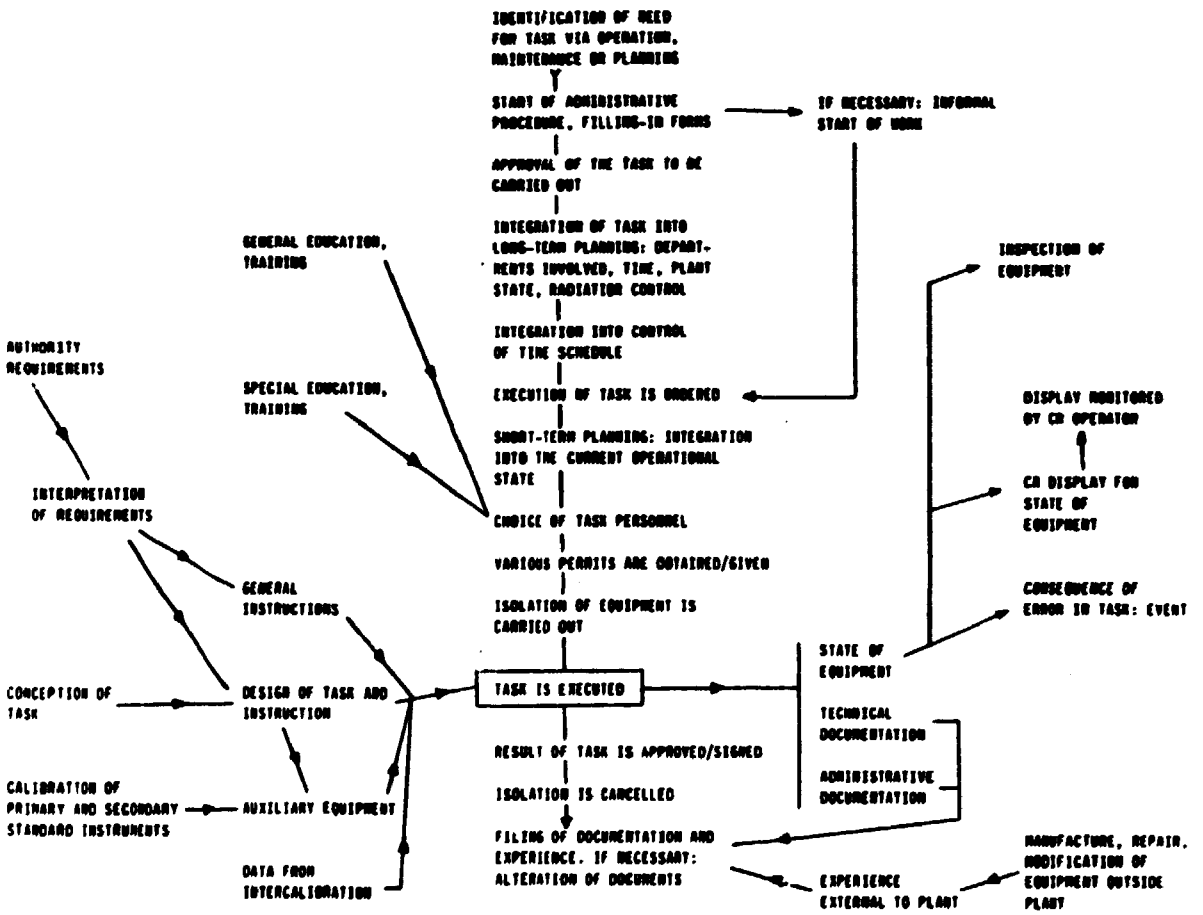


Figure 2.2: Activities related with a test or calibration task.

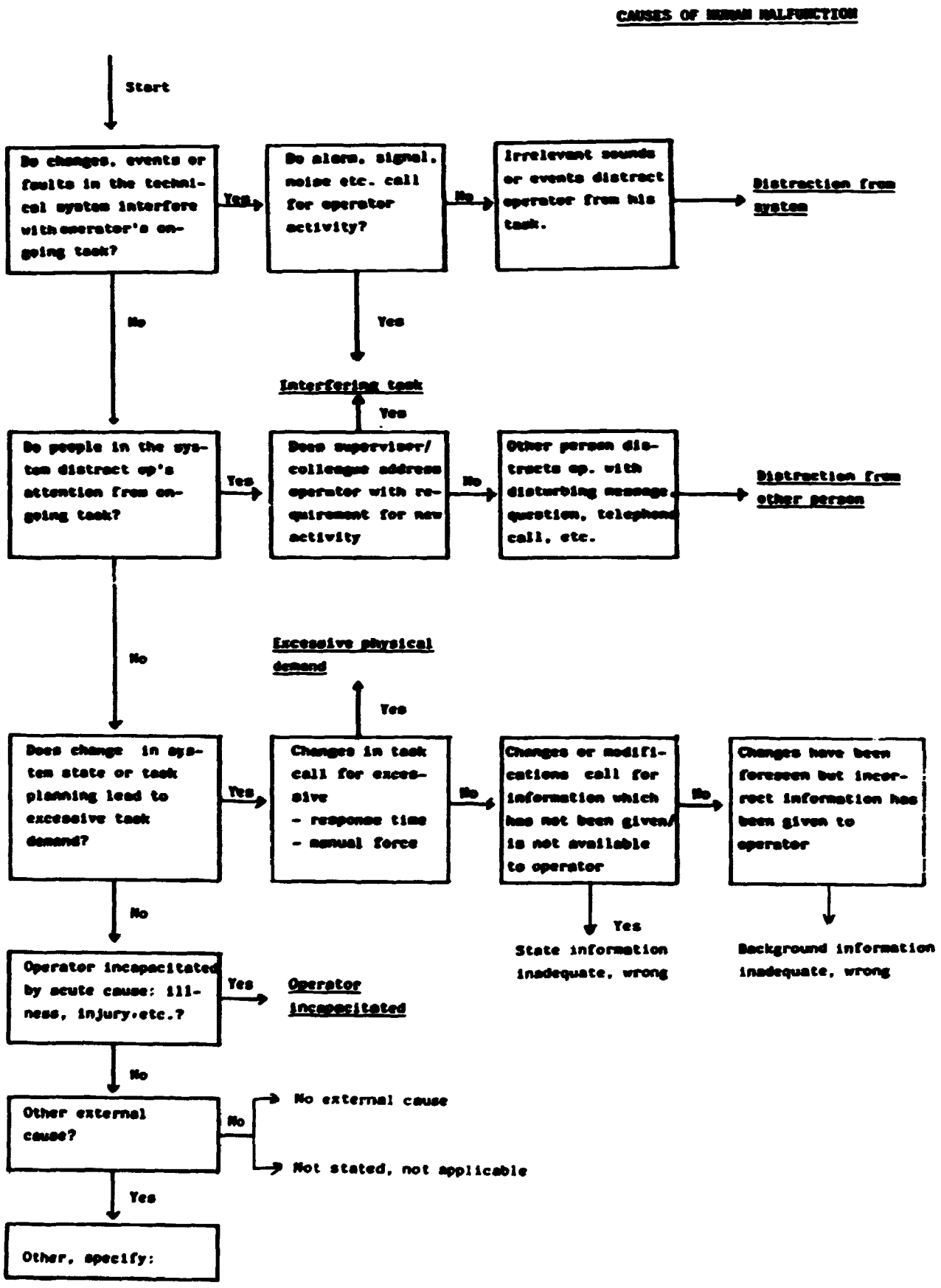


Figure 2.3: Guide for using the category: Causes of Human Malfunction

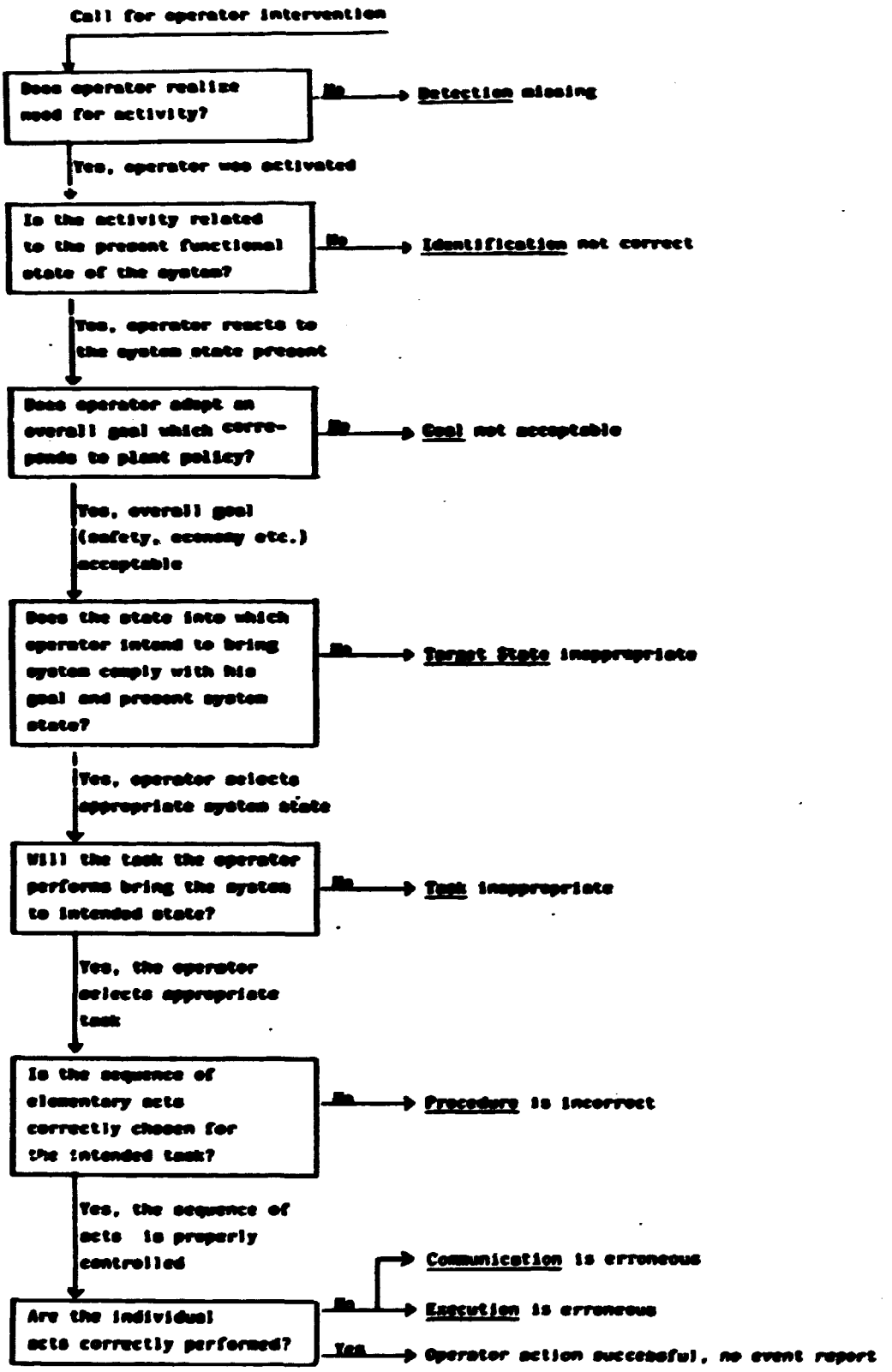


Figure 2.4: Guide for using the category: Internal Human Malfunction

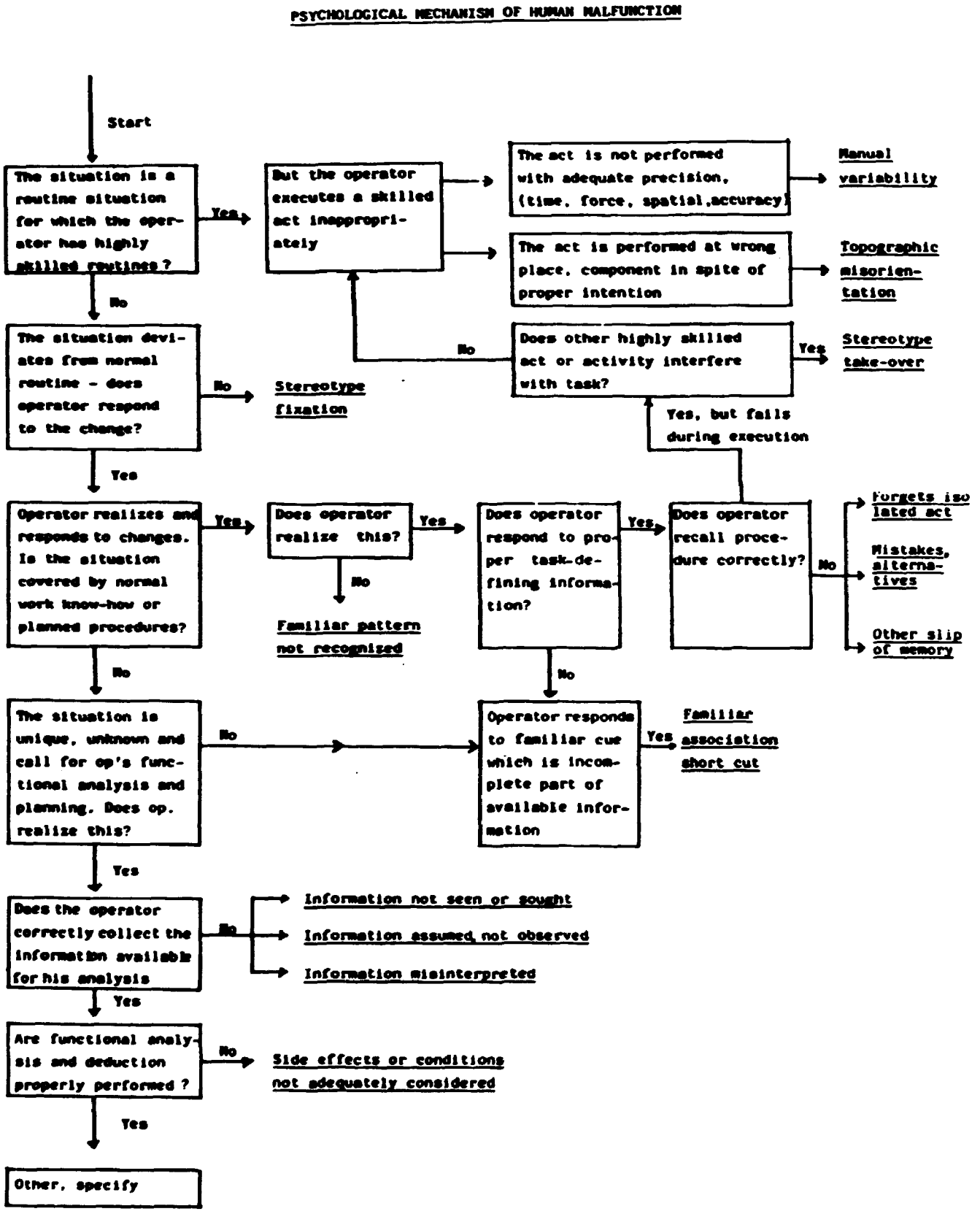


Figure 2.5: Guide for using the category: Psychological Mechanism of Human Malfunction

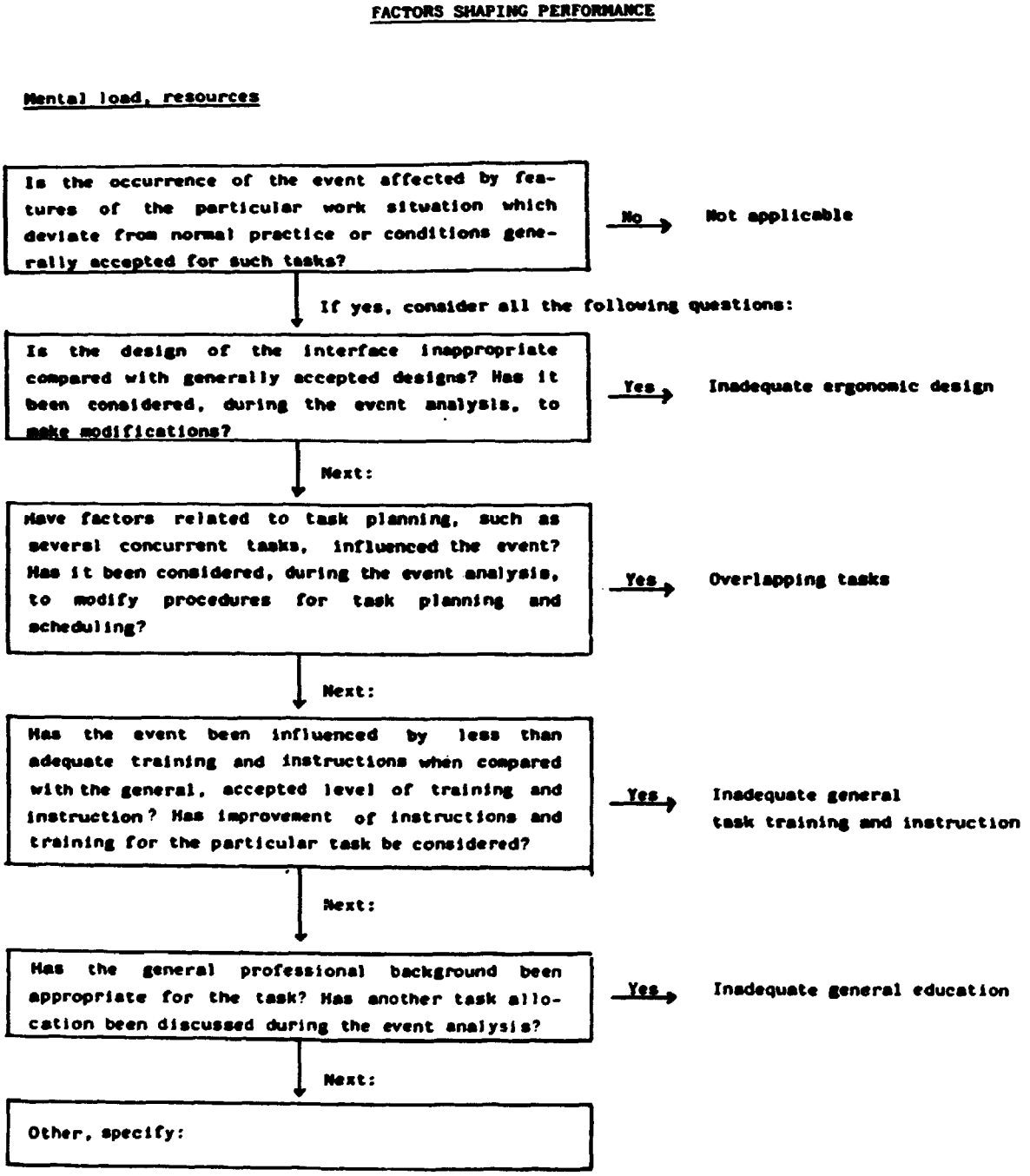


Figure 2.6: Guide for using the category: Factors Shaping Performance, Mental Load, Resources

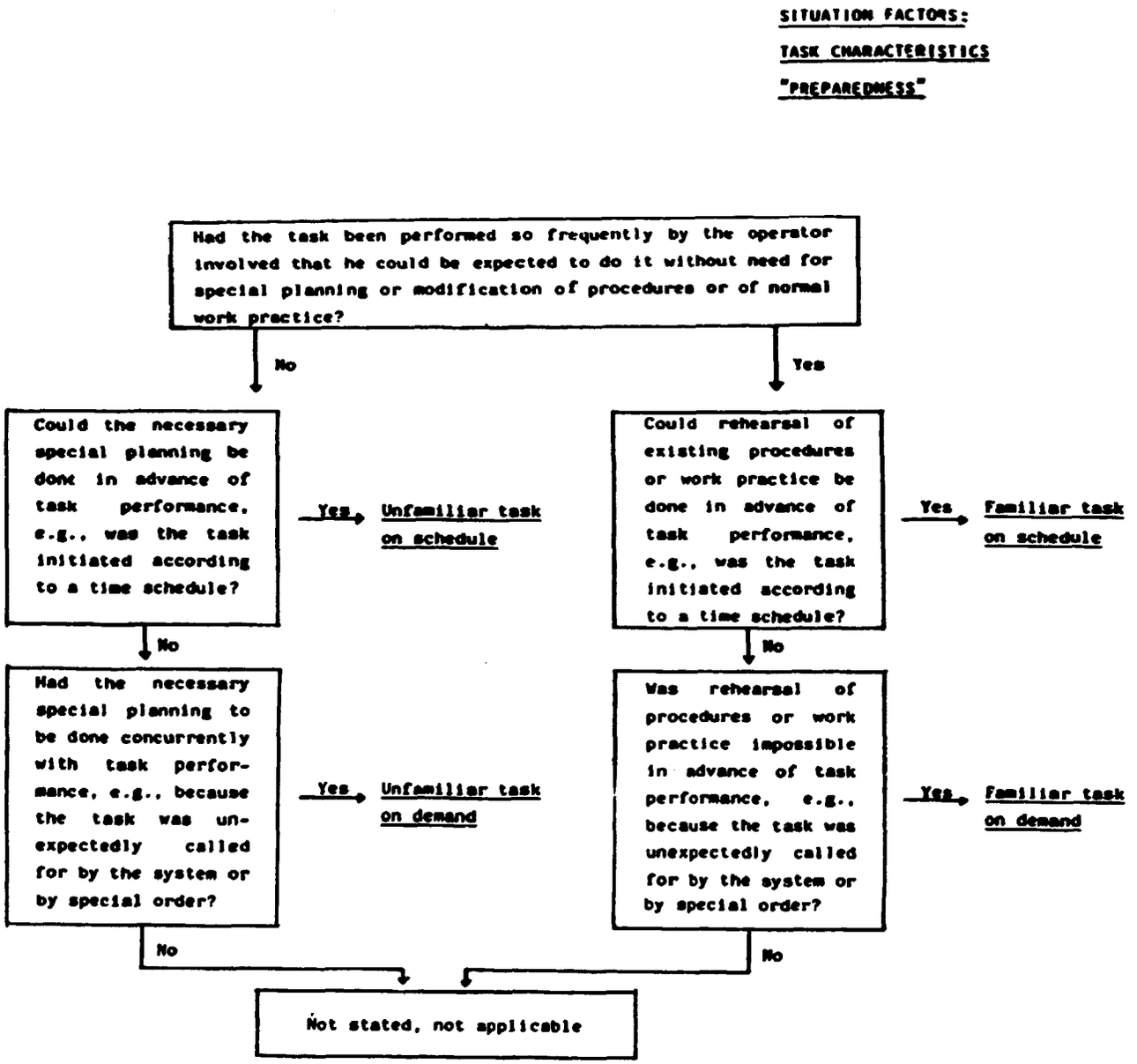


Figure 2.7: Guide for using the category: Situation Factors, Task Characteristics, "Preparedness".

3. WORK ANALYSIS: PRE-IDENTIFICATION OF HUMAN RISK CONTRIBUTIONS IN SCHEDULED, FAMILIAR TASKS

In section 2 the use of the description system for post-incident analysis has been described. Post-incident analysis implies a breakdown of the incident into the features given by the description system of Appendix A, and the quality of the system is related to the extent to which the causal flow and the mechanisms controlling the event propagation are maintained and can be regenerated from the data. When used for pre-identification of errors, the description system must serve a synthesis of relevant, possible chains of events due to human malfunction utilizing the descriptors contained in the categories together with a ranking of the significance of the possible events.

The method: Work Analysis (WA), presented in subsection 3.1., is, in its present form, intended for supporting the design of scheduled, familiar tasks and the improvement of existing tasks and for providing documentation of risk-related intentions in task design and modifications.

The WA has been developed with the intention of serving the integrated PRA/RM concept mentioned in section 1. The application of WA to this purpose is treated in subsection 3.2. at a rather general level describing how the method should be incorporated in the procedure of providing a PRA. Finally, subsection 3.3. presents some preconditions necessary for quantified prediction.

3.1. Work Analysis Applied to Task Design and Improvement

Work analysis is intended for the pre-identification and counteraction of errors in scheduled, familiar tasks with unchangeable procedure, i.e. errors owing to "normal human variability" in skill- and rule-based activities.

However, more detailed and precise criteria are wanted for guiding the decision as to whether a given task design is

accessible to formal analysis. For the present state of the art this lack of criteria can to some extent be compensated for by careful recording, during the WA, of everything met with which constitutes a necessary condition for the analysis to be valid. This will also support a delimitation of the task to be analysed relative to adjoining activities to be omitted and therefore to be taken care of otherwise.

A rule-based task supported by written instruction is likely to develop into a task totally skill-based and with its instruction recalled by heart: This should be foreseen in task design by providing error recovery possibilities also covering this change in level of behaviour and followed up by observation of actual task performance and feedback of experience. Also, for the purpose of error detection, it may be important to maintain knowledge, even though high skill is developed, as discussed in subsection A.2.

Tasks which are not suited for WA could be treated in one or more of the following ways:

- By converting the task to a technical activity, e.g. by automation, with predictable risk contribution and supplemented by human maintenance activities covered by WA.
- Administrative precautions against errors to be established during task performance, the efficiency of these precautions to be controlled by RM utilizing feedback of experience.
- By securing that the error effects are reversible and subject to predictable error detection and correction functions.

3.2. Overview

Identification of the possibilities of human malfunction in a task considered in isolation is not very meaningful. The basis for any human error identification in the present context will be the results of a functional analysis of the technical system or the task environment including a technical failure analysis. This analysis will serve to identify the requirements for human involvement and to specify these requirements in terms of plant-oriented activities and involved components required to

bring the technical system from one state to another. The term "task" is designated to this set of activities and components.

Also, the technical failure analysis, in case of attempting quantified prediction, could provide probability estimates for the relevant equipment failures and other not human-caused events, such estimates will be very useful to serve as stop rules to prevent unnecessary deep search for human error mechanisms.

When the task requirements have been formulated in plant--oriented terms they should be connected with the description system for human malfunctions as indicated in Fig. 3.1. The problem now is to describe the activities in human-oriented terms, i.e. to determine for each activity which "internal mental function" is required by the activity and could be wrong. Or it may be necessary to further subdivide the activity until application of this category is possible.

Next, candidate "psychological mechanisms" are postulated for leading to erroneous "mental function", the selection of candidate mechanisms can be supported by postulating "external causes" and "human factors" influences specific for the given task and its circumstances. The effect of the erroneous mental function upon the activity performance can then be determined in detail, leading to identification of relevant "external modes of error". Finally, the related specific fault trees can be constructed.

Example: If we consider as a simple example the activity of closing a valve, this can be unsuccessful due to different "psychological mechanisms". It may be opened fully instead of closed due to "mistake of alternatives" or due to "stereotype fixation" (if its operation appears in reverse to usual). Closing may be omitted due to simple "slip of memory", the omission being more likely if the activity is "functionally isolated" from the main course of the task. Or a wrong valve may be closed, in which case we have two error effects, perhaps with coupling between them, and it is important to predict the mistaken valve. Depending

upon the mechanism involved, this valve may be topographically close ("topographic misorientation"), have a name or label which can be mistaken ("mistake of alternatives", A for B for instance) or be part of a very familiar routine which is similar to the present activity (psychologically close, "stereotype take--over"). The message of this simple example is that, by postulating this human-oriented error chain, the causal relationship among mechanisms, mental function and task elements must be maintained when identifying the external mode of error in order to make possible the incorporation of the method into probabilistic risk prediction where the conservation of causality is a necessity.

When the effect of the errors and the potential for error recovery are identified in subsequent analysis, the candidate causes of errors are evaluated for their significance for lack of task result and for coupling to other events, and finally a quantified assessment may be attempted if needed.

Based on the description system general formats can be developed in order to aid the systematic identification of relevant human error chains and also for providing documentation of the analyst's search. Example formats are given in Figures 3.2 and 3.3.

3.3. Detailed Procedure

WA is analysis of reliability and immediate risk from performance in a familiar, well trained task which is part of a planned work schedule. This means: the goal or target of the activity is generally accepted; the cues to start of the task are known and, therefore, no errors of intention are considered.

The analyst should presume the existence of Risk Management with experience fed back from post-incident analysis and also should, during the entire analysis, record, when found, assump-

tions and preconditions to be fulfilled for the analysis and its results to be valid and to remain valid.

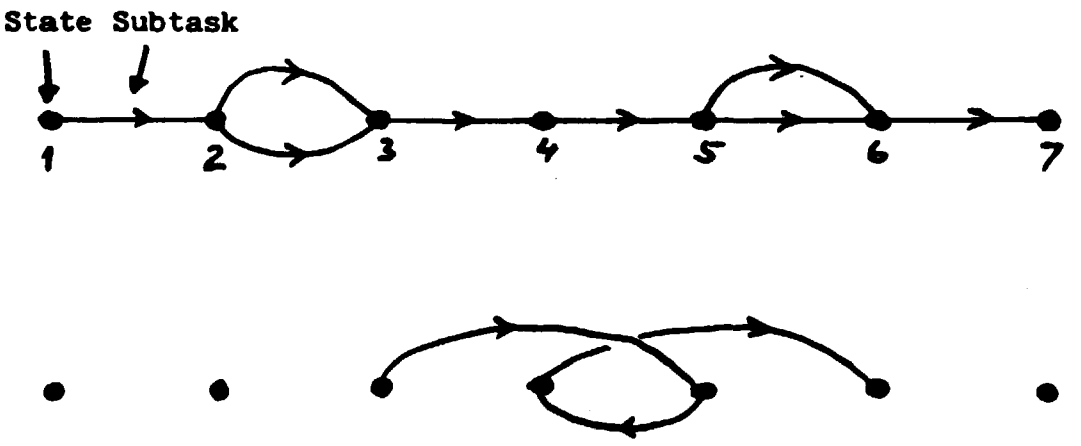
Also recorded should be cases where postulated data or information have to be used in order to have the analysis carried through in spite of lacking data or information.

a. Analysis of Task Sequence

Use instructions and manuals as well as interviews and observations.

a.1. Define a sequence of phases or subtasks which is determined by functional requirements of the system and which cannot be modified without interrupting the task.

a.2. Define the necessary acts of the different alternative, functionally acceptable action sequences for each subtask, (i.e., also possible short-cuts, tricks of the trade, which lead to an acceptable result).



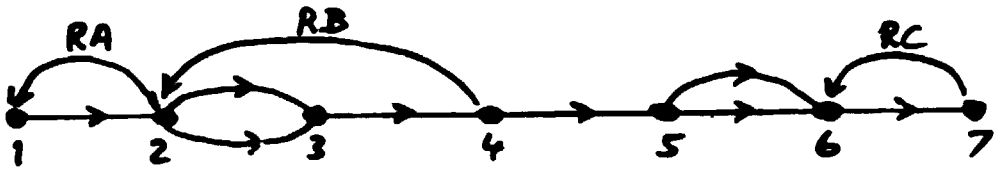
Example: Alternative sequence

b. Analysis of Task Reliability

b.1. Define acceptance criteria for task result. (Criteria for task process are related to analysis of risk).

b.2. Define error recovery points; i.e., define points in the sequence in which previously committed errors will be

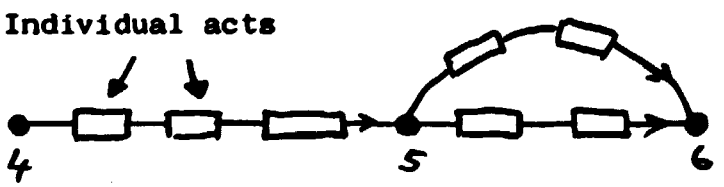
immediately observable and reversible - either directly observable or because task sequence is interrupted as a consequence of the error, making subsequent action difficult. (Such recovery points may correspond to links between subtasks of a.1.).



Error recovery paths found: RA, RB, RC.

b.3. Define those acts or action sequences for which the influence on task result is not covered by error detection and recovery; i.e., errors will not be observable and reversible.

b.4. For these acts, identify the human error modes which will lead to uncorrected, unacceptable task result.



This error-mode-and-effect analysis can be performed by postulating errors in terms of external acts only or by also including postulated psychological error mechanisms, i.e. by

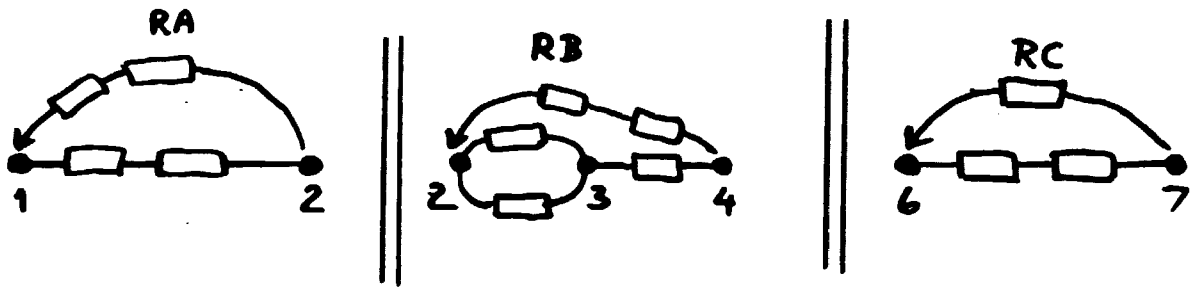
involving the human malfunction description system as indicated in Figure 3.1.

The first type of analysis is the simplest; however, in risk analysis the latter is preferable.

The example formats of Figures 3.2 and 3.3 could support postulation and documentation of the errors found relevant.

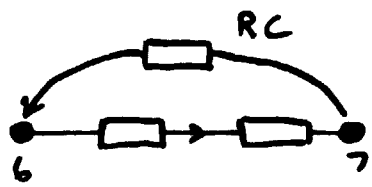
The formats are applied to each individual act, one sheet of the format showing those action errors and the corresponding mechanisms found relevant for a particular act.

b.5. Evaluate conditions for error detection and correction at the states found in b.2. Define error modes which will cause unsuccessful error recovery.



b.6. Apply human error rate estimates to evaluate total task reliability, considering errors and modes found in b.4. and b.5.

For b.5., as an example:



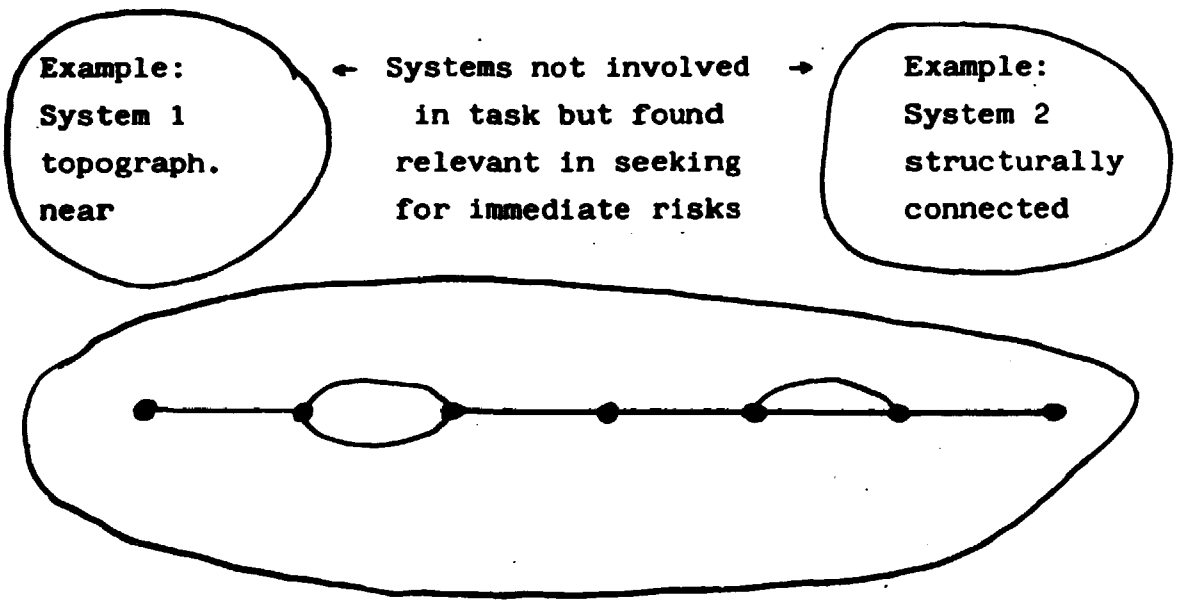
If error probability for the string 6 to 7 is 1/10 and for RC 1/10, then the resulting error probability in obtaining state 7 from state 6 is 1/10 x 1/10 = 1/100.

b.7. Judge whether the reliability of the error recovery at the recovery points of b.2. is in fact sufficiently high to ignore errors in the preceding sequence.
If not, repeat b.3. for these sequences.

Are RA, RB, and RC enough reliable?
If not: Neglect those RX considered unreliable. For the corresponding non-recoverable sequences repeat b.4. and b.6.

c. Analysis of Immediate Effects

c.1. Define the topographically nearest as well as the structurally and functionally connected systems which can be affected by erroneous human acts.



System involved in task

The information needed for defining the task-external systems should be stated. This information is not to be expected given in the conventional functional descriptions.

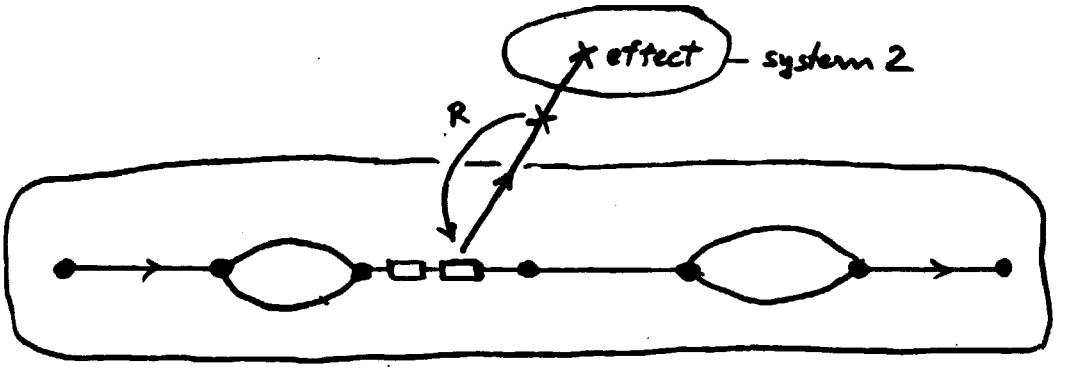
c.2. Define the set of error modes which should be used in an error-mode-and-effect analysis. Connect modes with psychological error mechanisms in order to be able to perform c.6.

c.3. Apply this set of postulated errors for each of the steps in the applicable task sequences of a.2.

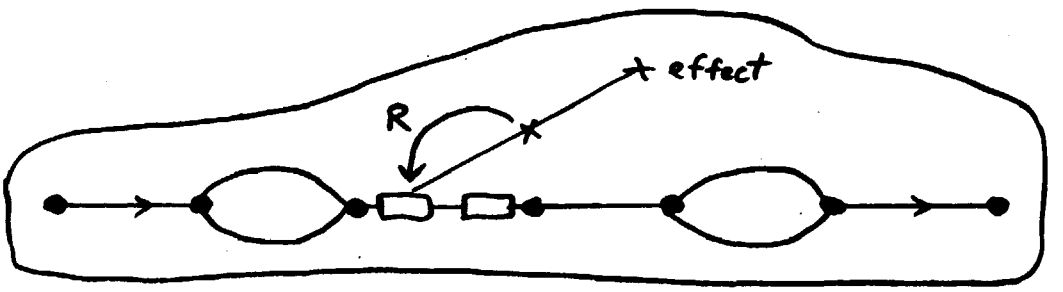
Again the formats of Figures 3.2 and 3.3 can be used.

c.4. For each action and error mode, identify possible unacceptable effects on the system worked on, as well as those systems identified in c.1.

c.5. Judge possibilities of error detection and recovery for each relevant error mode from c.4. (These possibilities are, generally, different from those under b.5.).

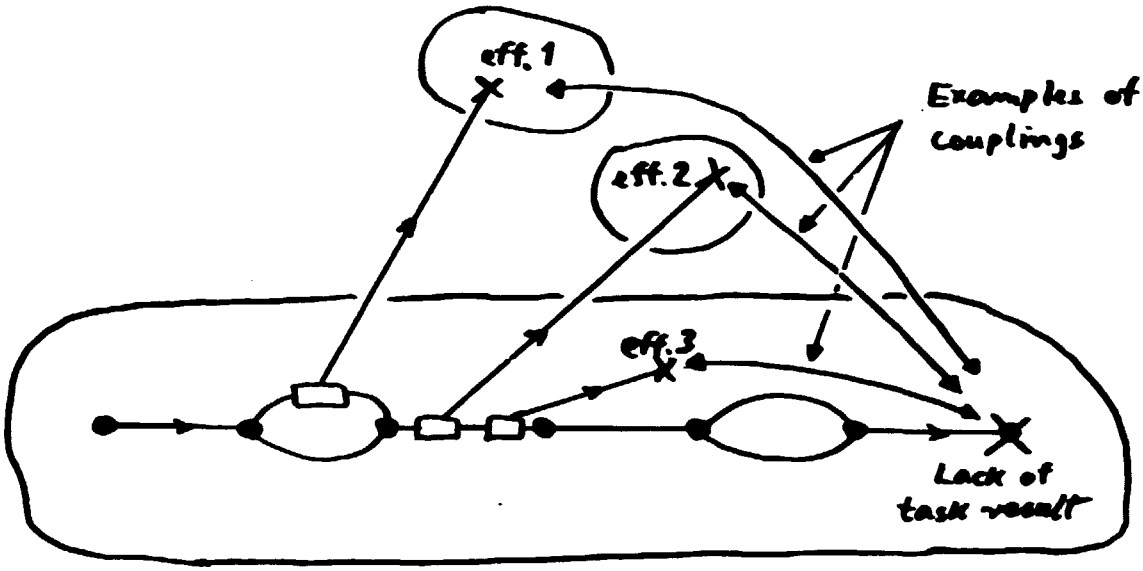


Example



Example

c.6. Evaluate the significance of the possible simultaneous presence of an erroneous act and an unacceptable task result, i.e. a possible, systematic coupling between two abnormal chains of events.



c.7. Categorize unacceptable effects found by c.4. and c.6. in relation to the overall risk analysis as given in the Cause Consequence Charts.

c.8. Apply human error estimates for the significant contributors in c.4. and c.6.

d. Analysis of Task Disturbances

Task disturbances may lead the performer to re-evaluate the task conditions. This may result in decisions which, if erroneous, may give human "errors of intention".

d.1. Evaluate sources of disturbances. Define the categories to be analysed in an explicit way. Formulate assumptions in order to facilitate "risk management" of those assumptions not included in the analysis.

Examples of typical sources of disturbances:

- personnel/work planning and scheduling
- tools/equipment; materials, spareparts
- latent, faulty conditions in system worked on.

d.2. Identify for each of the task steps not covered by error recovery and for the error recovery path, the possible lack/degradation of planning/tools/material/information which will affect task conditions.

d.3. Identify the normal, typical, easy alternative replacements or improvisations of the particular profession and work setting.

d.4. For the improvised task sequences identified in d.3., repeat analysis under a., b., and c. If effects are unacceptable and conditions too unstructured for analysis, modify system or specify risk management.

3.4. Work Analysis Utilized in PRA

As explained in section 1 WA is developed in order to satisfy the requirements to be demanded if the method efficiently should fit into the integrated PRA/RM concept. These requirements are discussed in ref. 1, and so is the incorporation of WA into an overall plant PRA.

The following general procedure is assumed for the incorporation of WA into an overall plant PRA:

Firstly, a basic PRA is performed for the plant technical systems and for those human activities which are contained in the formalized and instructed operator tasks, i.e. such human activities have been subject to Work Analysis covering the human reliability and the immediate risk from human errors during performance of formally instructed activities. A set of criteria must be established to guide the decision as to whether a given task design is acceptable for formal analysis and it is assumed that identification of necessary human activities not corresponding to such criteria will lead to modification of the system design. In our view, with the present state of the art, only scheduled, familiar tasks are considered to be accessible to formal analysis. Fig. 3.4 gives an overview of the content of a WA and its relationships to the cause-seeking strategy of risk analysis. The failure analysis

of the technical systems should provide probability estimates for the relevant equipment failures and other events not caused by humans, such estimates will be very useful by serving as stop rules to prevent unnecessary deep search for human errors.

Secondly, as a supplement to the basic PRA, an analysis is performed of the possible modifications of the PRA content owing to errors during human activities in general. Important types of human interferences are those that will

- affect the frequency of event chains,
- change the structure of event trees by breaking the recovery paths representing protective functions,
- introduce couplings between otherwise independent events.

Search strategies for the identification of such interferences still have to be developed, proposals are given in ref. 1, where also are discussed the properties of the risk analysis to be required for the PRA/RM concept to be efficient.

3.5. Quantification of Human Risk Contributions

The concise statements from ref. 4 are still valid as criteria for meaningful quantitative human factors assessment of reliability and safety and hence are quoted in the following:

Properties characterizing the human as part of a system:

- Man is adaptive and able to learn and therefore may inappropriately respecify a function or a task.
- Man may be occupied by several tasks simultaneously.
- Man may respond to total situations rather than to individual events or system states.
- Man is influenced by factors badly defined and difficult to quantify, such as motivation, stress, fatigue, etc.
- Several different internal mental functions of man can serve the same external function, depending on his training and skill, prior experiences, subjective criteria etc.
- Man is capable of selfmonitoring and error correction.

Conditions for reliability analysis including human malfunctions:

Reliability is defined as the ability to maintain a specified, wanted function. Quantification leads to figures describing the probability that a specified wanted function will be performed e.g. during a given time.

Due to the particular properties of man mentioned above a systematic analysis and quantification of system reliability is not feasible unless the design of the system and the work situation of its operators satisfy some general conditions. Necessary conditions for the use of probabilistic methods to predict the probability that a specified task is performed satisfactorily by human operators are:

- There is no significant contribution from systematic errors due to man's inappropriate redefinition of task, interference from other tasks or activities, etc.;

and

- The task can be broken down to a predictable sequence of separate subtasks at a level where failure data can be obtained from similar work situations, i.e. the task is performed in the rule-based behavioural domain

and

- These independent subtasks are cued individually by the system or by other external means, so that modification of procedure does not take place;

or:

- If these conditions are not satisfied, e.g. because the task is performed as one integrated whole, or it is performed by complex and variable human functions such as higher level cognitive functions, then the effect of errors in the task must be reversible and subject to an error detection and correction function, which in turn satisfies the above-mentioned conditions for predictability. A lower bound on the total reliability can then be derived from the frequency of opportunities for error and the reliability of the error-correcting function.

Conditions for safety analysis
including human malfunctions:

Safety is defined as the ability to prevent losses in consequence of accidental maloperation not only due to the absence of wanted functions but also due to the occurrence of unwanted/unexpected, particularly human, functions and to combinations of these types of functions.

Again, due to the properties of man, a systematic analysis and quantification of specific consequences of accidental events in a system can only be quantified if:

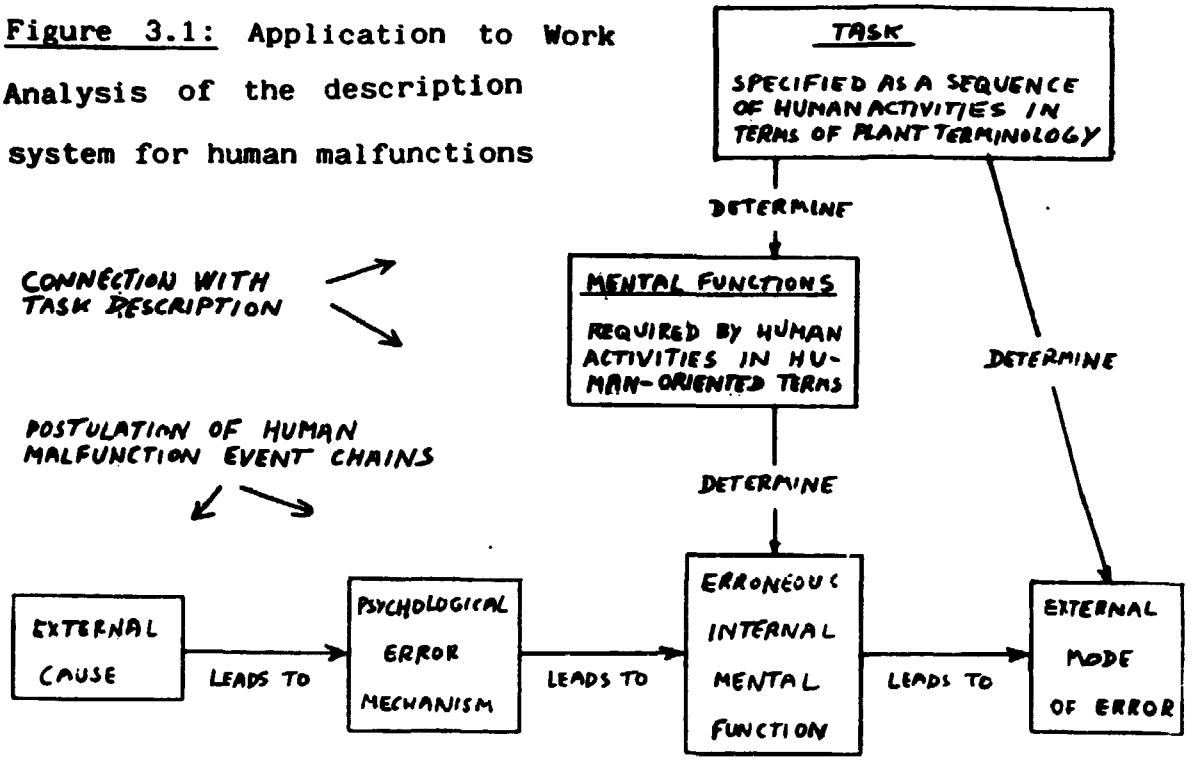
- it can be demonstrated that the effects of erroneous human acts are not significant contributors to the probability, if necessary by introduction of interlocks or barriers which prevent human interaction,

or

- the effects of erroneous human acts are reversible and detectable by a monitoring or safety function which can be performed by operators or automatically.

If the reliability of such barriers and safety functions can be quantified then an upper bound of the probability of the event in question can be derived from the frequency of error opportunities.

Figure 3.1: Application to Work Analysis of the description system for human malfunctions



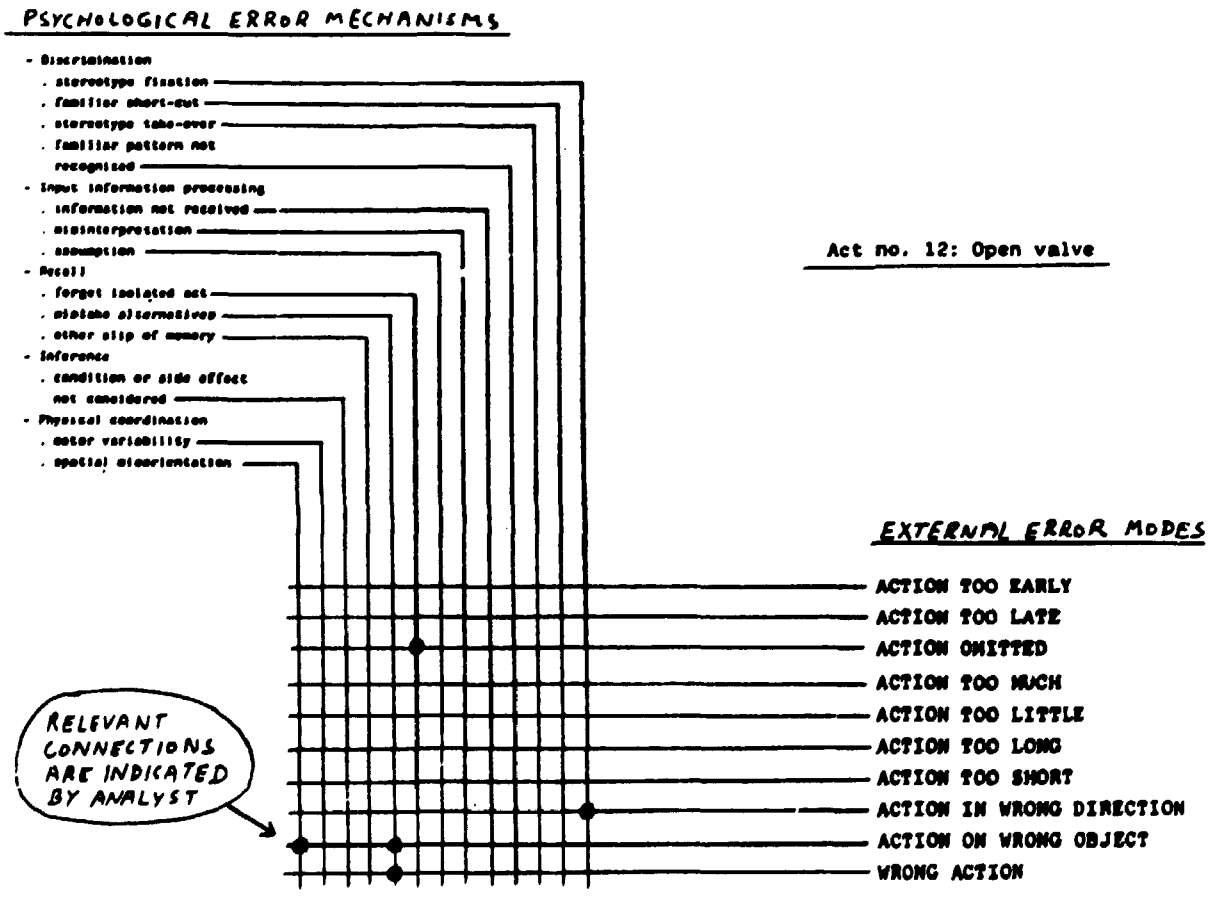


Figure 3.2: Systematic postulation of errors: Example format.

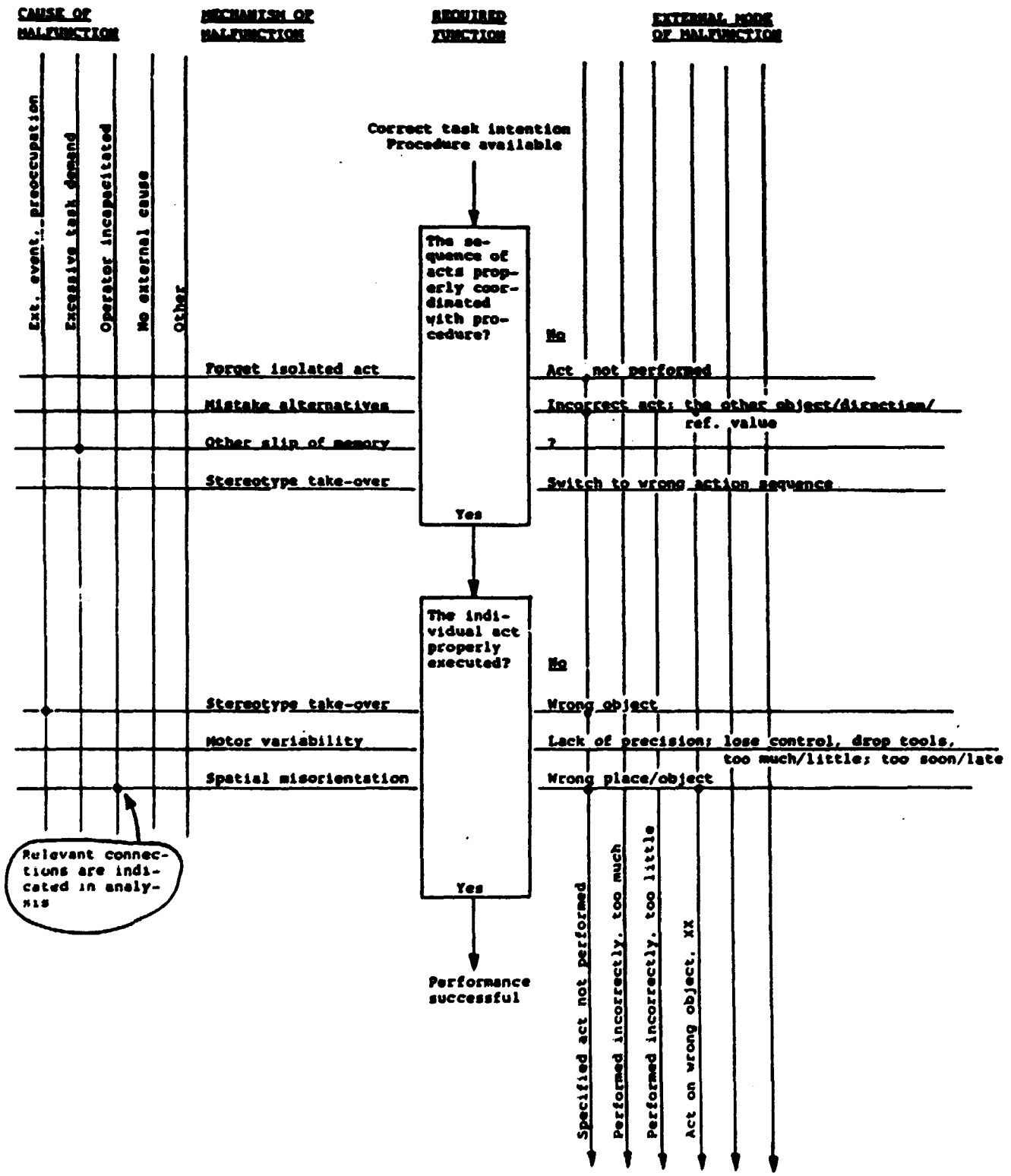


Figure 3.3: Systematic postulation of relevant errors: Example format. For illustrative purpose, only limited numbers of items in the different categories are included.

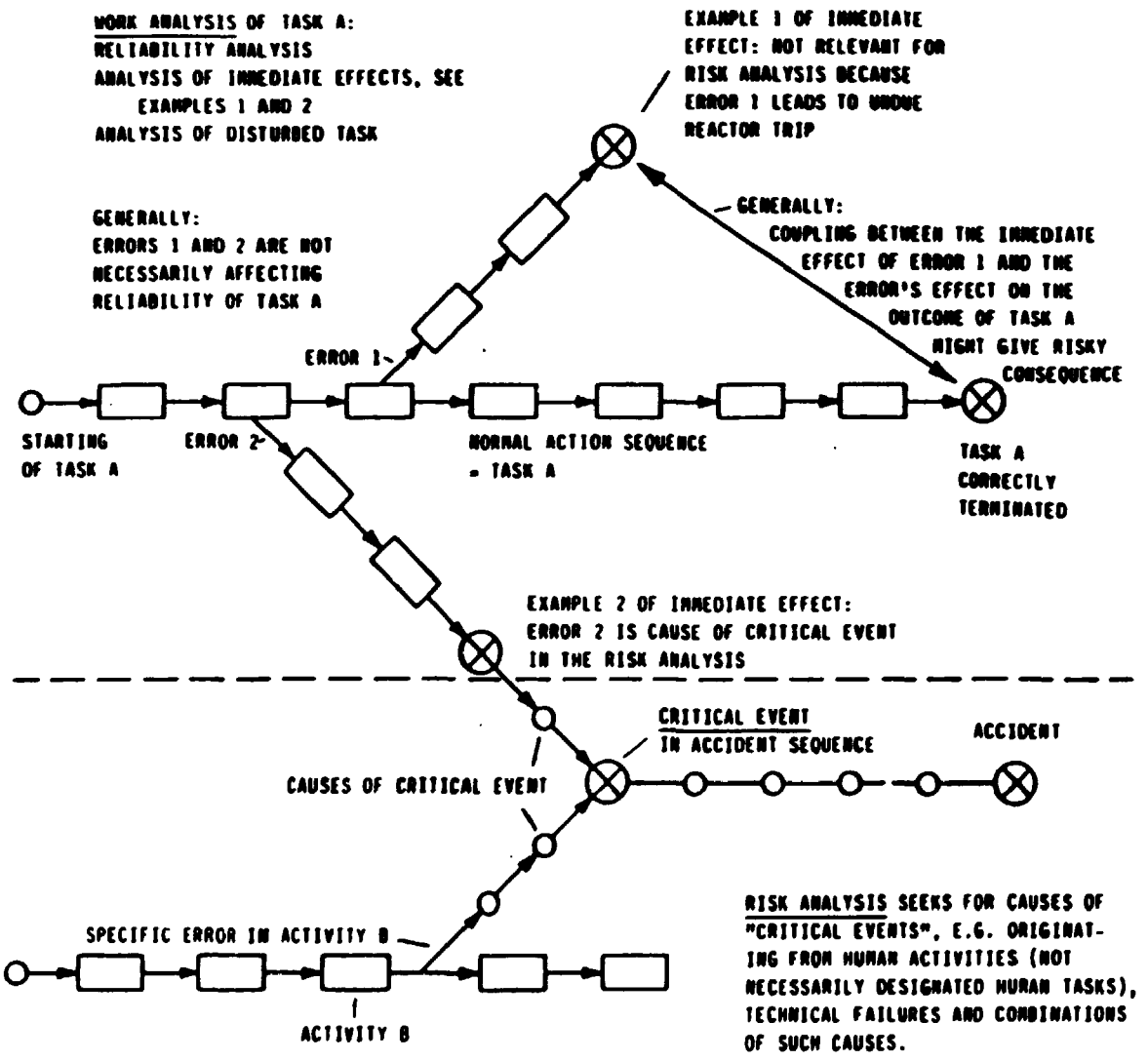


Figure 3.4: Illustrates the difference between the search strategies applied in Work Analysis: with starting point in normal work sequences and seeking for the effects of errors, and in Risk Analysis: with starting point in a critical event seeking for its possible causes among technical failures and human activities and errors.

APPENDIX A: The Description System for Human Malfunctions

A.1. Outlines of Description Categories

The description system used in common for the predictive analysis and the post-incident analysis is shown in principle in Figure A.1, referred to in the following.

The box "personnel task" is representing the description of the task in question, e.g. an operational task, and is in terms of the human interactions with the technical system, e.g. as given by a written instruction. Each step of the detailed task description, e.g. "press button", corresponds with a descriptor in the box "internal human malfunction". The descriptors of this box are in generic human-oriented terms not specific for the task considered and should answer the question: which kind of internal mental function did fail?

Each step of the task description also determines how the erroneous performance of this step can manifest itself as an observable external effect as given by the descriptors in the box "external mode of malfunction".

It should be noticed that the contents of "internal human malfunction" have been developed particularly for control room operator activities and could be modified for better coverage of other task types. Similarly, the contents of "external mode" could be extended and/or adapted to specific task types.

The category "psychological mechanisms" describes the psychological error mechanisms which influenced that internal mental function which was inappropriately performed. The descriptors have been found to cover the larger part of the more simple cases, however, could be expected supplemented with further mechanisms found by post-incident application of the description system.

The box "causes of human malfunction" describes causes of the initiation of the psychological mechanism whether external or attributed to the human. Again the contents should be considered an example and adaptable to specific applications.

More general influences upon the task are covered by the descriptors in "factors affecting performance" and "situation factors", since they do not themselves release a chain of events but modify the probability of having a chain released by other causal events.

The important properties of the description system are that the four categories in the lower part of Figure A.1 enables the analyst

- in post-incident analysis to identify a causally ordered chain of descriptors connecting an external cause of the human malfunction with an external manifestation of the effect of the malfunction through two human-oriented descriptors of a general, not task-specific, kind,
- in predictive analysis to postulate relevant causally-ordered chains of the same kind as above and to generate relevant scenaria,
- to have the chain of descriptors connected with a conventional task description given in equipment-oriented terms.

Condensed flow-graph guidelines for use of the categories in post-incident analysis are given in section 2:

Causes of malfunction: Fig. 2.3
Psychological mechanisms: Fig. 2.5
Internal malfunction: Fig. 2.4
Situation factors, task characteristics, "preparedness": Fig. 2.7
Factors shaping performance, mental load, resources: Fig. 2.6.

The guides are intended particularly for control room activities, however, can be applied to other activities.

In the following are described in detail the two categories particularly human-oriented: Psychological mechanisms and internal malfunctions and also their underlying models.

A.2. Category: Psychological Error Mechanisms, and the "3-Level Model"

The category represents an attempt to formulate a set of generic, task independent human error mechanisms. To evaluate human performance during design of new tasks and for the improvement of existing work conditions, including man-machine interfaces, it is important to identify human malfunction mechanisms in generic terms relating inappropriate task performance to features of those psychological mechanisms which are the basis of the performance and to mechanism properties putting limits to performance.

A human is capable of performing the same task in various different ways depending upon the state of training, the subjective formulation of the goals and performance criteria, and consequently the role of the psychological mechanisms will be very dependent on person and situation. Inappropriate task performance reflects a mismatch between task requirements and the human resources applied, and if the nature of this mismatch can be identified - irrespectively of the underlying cause - important information on the psychological mechanism applied and its limiting properties with respect to the task can be obtained.

The present category is intended to characterize cases of such resource/demand mismatch and is based on a model of operator performance derived from a preliminary analysis of 200 Licensee Event Reports (ref. 2). The structure of the model is illustrated in Figure A.2.

Referring to Fig. A.2, human behaviour is considered subject to three different levels of control, the levels of skill-, rule-, and knowledge-based behaviour.

Skill-, rule- and knowledge-based behaviour are not alternative human processes; they are types of behavioural control which are probably all active at all times: Knowledge-based behaviour may comprise as ingredients also rule- and skill-based behaviour and rule-based behaviour may comprise skilled activities. During familiar work situations, when a rule-based activity is

controlled by know-how and automated subroutines, the conscious mind has time left for other business, which may be to plan the future, to monitor the effects of past activities, or to speculate on private troubles. The degree to which people tend to use knowledge-based functional reasoning to monitor their activities during familiar work situations probably depends very much on one's individual disposition, but the opportunity to do so certainly also depends on the man-task interface design.

The skill-based behaviour represents sensori-motor performance during acts or activities which, following a statement of an intention, take place without conscious control as smooth, automated and highly integrated patterns of behaviour.

At the skill-based level the perceptual-motor system acts as a multivariable, continuous control system synchronizing the physical activity such as navigating the body through the environment and manipulating external objects in a time-space domain. For this control the information is perceived as time-space signals, continuous, quantitative indicators of the time-space behaviour of the environment. These signals have no "meaning" or significance except as direct physical time-space data. The performance at the skill-based level may be released or guided by value features attached by prior experience to certain patterns in the information, these patterns not taking part in the time-space control but acting as cues or signs activating the organism. Performance is based upon a very flexible and efficient dynamic internal world model.

At the next level of rule-based behaviour, the composition of a sequence of subroutines in a familiar work situation is typically controlled by a stored rule or procedure which may have been derived empirically during previous occasions, communicated from other persons' know-how as an instruction or cookbook recipe, or it may be prepared on occasion by conscious problem solving and planning. The point is here that performance is goal-oriented, but structured by "feedforward control" through a stored rule. Very often, the goal is not even explicitly formulated, but is found implicitly in the situation

releasing the stored rules. The rule or control is selected from previous successful experiences and evolves by "survival of the fittest" rule. Furthermore, in actual life, the goal will only be reached after a long sequence of acts, and direct feedback correction considering the goal may not be possible.

At the rule-based level, the information is typically perceived as signs.

During unfamiliar situations, for which no know-how or rules for control are available from previous encounters, the control of performance must move to a higher conceptual level, in which performance is goal-controlled, and knowledge-based. In this situation, the goal is explicitly formulated, based on an analysis of the environment and the overall aims of the person. Then a useful plan is developed - by selection, such that different plans are considered and their effect tested against the goal, physically by trial and error, or conceptually by means of understanding of the functional properties of the environment and prediction of the effects of the plan considered. At this level of functional reasoning, the internal structure of the system is explicitly represented by a "mental model" which may take several different forms. To be useful for causal functional reasoning in order to predict or explain unfamiliar behaviour of the environment, information must be perceived as symbols.

During training in a particular task, control moves from the knowledge- or rule-based levels towards the skill-based control, as familiarity with the work scenarios is developed. An important point is that it is not the control processes of the higher levels that are automated. Automated manual skills are developing while they are controlled and supervised at the higher levels. When explicit knowledge or rules are no longer needed for behavioural control during normal work, they will eventually deteriorate. With respect to error observability, it is a problem at the skill- and rule-based levels that the goals are not explicitly controlling the activity. This means that errors during performance may only be evident at a very late stage - an error in the use of a recipe may not manifest itself

until you taste the cake, i.e. when the product is present. Early detection of the effect of one's own variability (or of changes in system conditions) depends on an ability to monitor the process, i.e. on knowledge-based monitoring based on understanding of the underlying processes. For error detection it may therefore be important to maintain knowledge, even though high skill is developed.

In Fig. A.2 is indicated how the psychological error mechanisms are associated with the 3-level model and in the next paragraph the mechanisms will be explained in detail.

A.3. Descriptors of the Category: Psychological Error Mechanisms

DISCRIMINATION

This group is related to the man's ability to discriminate between levels of control needed for his activities and select the proper level for each activity. The subcategories of mechanisms are characterized by interference between the man's repertoire of stereotyped habitual - and often subconscious - responses on one side and on the other side aspects of the actual work situation during infrequent and unique task demands.

Stereotype (skill) fixation: Man operates in skill-based domain. He does not recognize a situation calling for attention and caution. (Cues for recognition may not be present or may be overlooked, this is characterized by the categories: Cause of Human Malfunction or Internal Human Malfunction).

Stereotype fixation represents the situation when a skill-based activity is activated or continued in an improper context, and the person on afterthought very well knows what he should have done. He does not switch to proper rule-based control.

Examples: - An operator presses air out of a plastic bag containing dust in order to seal it, although he knows it contains radioactive material. He gets contaminated in the face.

- During a clean-up operation in a radioactive area, a vacuum cleaner fails. A foreman opens it for a possible rapid repair, despite the fact that he knows it contains radioactive dust.

In both cases, normal everyday reactions are carried over to a special context. Also this appears to be a reasonable and effective learning mechanism - in a reversible context. Here the unvisible radioactivity makes the environment "unkind".

Familiar association short-cut: It is recognized that conscious identification of the situation is needed but familiar cues activate incorrect intention and task in man. It is not recognized that knowledge-based evaluation and planning is needed. Transfer from rule- to knowledge-based control is impeded.

There is a considerable probability of highly skilled operators with a large repertoire of convenient signs and related know-how not switching to analytical reasoning when required, if they find a familiar subset of data during their reading of instruments. They will rather run into a "procedural trap" and be caught by "familiar association short-cut" very probably based on a subset of the available data. Examples from major industrial incidents are numerous.

Stereotype take-over: Task or act according to proper intention, but "absentmindedness" during performance leads to relapse to stereotype action links related to different act or task.

A single conscious statement of intention may activate a proper familiar schema, whereafter the attention may be directed e.g. towards planning of future activities or monitoring the past. The current, unmonitored schema will then be sensitive to interference leading to "stereotype take-over", i.e. another schema takes over the control, either because a part of current action sequence is also part of another frequently used schema, or due to interfering intentions of the detached attention, i.e. transfer from a skill-based to a different inappropriate skill-based activity takes place.

Examples: - During normal operation of a process plant the power supply to the instrumentation disappears. Investigation reveals that the manual main circuit breaker in the power supply is in the off position. The conclusion was that a roving operator, checking cooling towers and pumps, inadvertently had swtiched from a routine check-round to the Friday afternoon shutdown check-round and turned off the supply. The routes of the two check-rounds are the same, except that he is supposed to pass by the door of the generator room on the routine check, but to enter and turn off the supply on the shutdown checks. Something on the way obviously had conditioned him for shutdown checks (sunshine and day dreams?). The operator was not aware of his action, but did not reject the explanation.

Lack of recognition of familiar patterns: Familiar pattern relevant for the situation is not recognized, higher level knowledge-based evaluation or planning is unnecessarily and inappropriately applied.

INPUT INFORMATION PROCESSING

The subcategories are related to the man's activities in obtaining information. (That an information malfunction has occurred is classified under: Internal Human Malfunction, erroneous function in action, communication given incorrectly).

Information not received/sought: Cues do not activate man because sensitivity/attention is insufficient for present information level.

Misinterpretation of information: Response is based on wrong apprehension of information such as misreading of text or instrument, misunderstanding of verbal message.

Assumptions replace search for information: Response is inappropriately based on information supplied by the operator (by recall, guesses, etc.) which does not correspond with information available from outside.

RECALL

Forgetting isolated item, act or function: Operator forgets to perform an isolated item, act or function, i.e. an act or function which is not cued by the functional context or is not having immediate influence upon the mental or motor sequence, or an item which is not an integrated part of a larger memory structure.

Mistake among alternatives: Simple choice of wrong alternative, a category is correctly used but by wrong member, e.g. mistakes of up/down, +/-, left/right, A/B, open/closed, locked/unlocked.

Examples:
- Using positive correction factors instead of negative; using increasing instead of decreasing signal in calibration.
- Disconnect pump A instead of B.

Other slips of memory: Erroneous recall of reference data values; names, item; need for actions, etc.

INFERENCES

This group is covering problems of linear thought in causal nets.

In present day control rooms based on individual presentation of the measured variables, the context in which operators make decisions at the knowledge-based level is far too unstructured to allow the development of a model of their problem-solving process, and hence, to identify typical "error" modes, except in very general terms, such as "lack of consideration in latent conditions or side effects" (ref. 2).

Side effects or latent conditions not adequately considered:
The man is in a less familiar situation characterized by knowledge-based, goal-controlled performance. He performs erroneously during functional inferences: The situation is not properly identified, the consequences of an event chain are not adequately predicted or an improper intention is chosen or latent conditions are not adequately considered. Consequently,

the task or the intended goal is not fulfilled or adverse side effects occur or a combination of these consequences. (Can be due to oversight, lack of knowledge etc., this is characterized by the category: Cause of human malfunction).

PHYSICAL COORDINATION

Motor variability: Lack of manual precision, too big/small force applied, inappropriate timing. Including deviations from "good craftmanship".

Examples:
- Inadequate precision leads to short-circuit of terminals with screw-driver.
- Inadequate precision in replacement of relay cover leads to short-circuit of relay terminals.
- Varying use of force in manipulating a bank of valves occasionally leaves a valve leaking.

Topographic, spatial orientation inadequate: In spite of man's correct intention and his correct recall of identification marks, tagging etc., he unawaringly performs task/act in the wrong place or on the wrong object, because he is following his immediate sense of locality, this, however, not being applicable (not updated, surviving imprints of old habits etc.).

Examples:
- A failure in one of several pump trains in the basement leads to the decision in the control room to switch off the "north train". However, during passage down stairs an operator looses orientation and switches off the southern train, even though he has the proper intention.

A.4. Category: Internal Human Malfunction, and the "Decision Ladder" Model

Ideally, the design of man-machine interface systems, particularly those utilizing modern information technology, should be based on a generic model of the information processes implied in the decisions to be taken by the control system including humans. To be generally applicable this model must be expressed in terms independent of the specific system and its immediate

control requirements. Unfortunately, such a generic model of the information processes implied does not exist.

The well-defined and well-structured nature of industrial process systems seems to be reflected in the supervisory control decisions in such systems: Studies of the activities in control rooms of fossil fueled power plants have led to the suggestion of a normative model in the form of a causally ordered sequence of necessary decision steps ("decision ladder") as shown in Fig. A.3:

First, the decision maker has to detect the need for his intervention and he has to look around and to observe some important data to have direction for subsequent activities. He then has to analyze the evidence available in order to identify the present state of affairs, and to evaluate their possible consequences with reference to the established operational goals and company policies. Based on the evaluation, a target state into which the system should be transferred is chosen, and the task which the decision maker has to perform is selected from a review of the resources he has available to reach the target state. When the task has thus been identified, the proper procedure, how to do it, must be planned and executed.

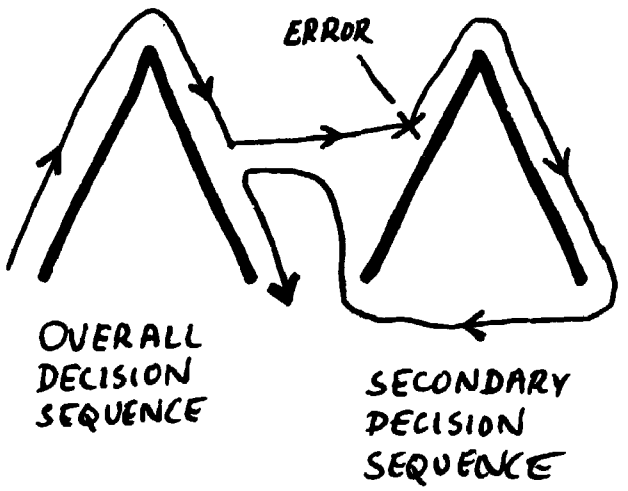
The nature of the information processes changes during the sequence. In the beginning it is an analysis of the situation to identify the problem, then a prediction and value judgement and, finally, a selection and planning of the proper control actions.

In Fig. A.3 is shown how in practice stereotyped processes can by-pass decision steps, this leading to very efficient performance. Also indicated is the relationship between the decision sequence and the "3 level model" of behaviour control in Fig. A.2.

It should be noticed that the breakdown of the decision task may result in different elementary phases if the task is belonging to systems not as well-defined as industrial process systems, e.g. social or administrative systems.

The "decision ladder" concept can be used on different levels within a given task. A repair task can be taken as an example: If we designate a "decision ladder" to the overall repair task and if the equipment failure is uncorrectly diagnosed, then the internal human malfunction will be erroneous "identification".

However, if the failure is correctly identified and the task of replacement properly mentioned but inappropriately planned because the internal state of the equipment is not properly identified at a more detailed level, then we have the following case: In the overall "decision ladder" the repair man performed error-free until his formulation of a procedure for the repair activities: In order to obtain a procedure he entered a secondary "decision ladder" for identifying the equipment details to be replaced. This "identification" belonging to the secondary "decision ladder" was erroneously performed, i.e. the error is in "identification" in terms of the secondary decision ladder and in "procedure" in terms of the overall decision ladder as visualized by the following figure:



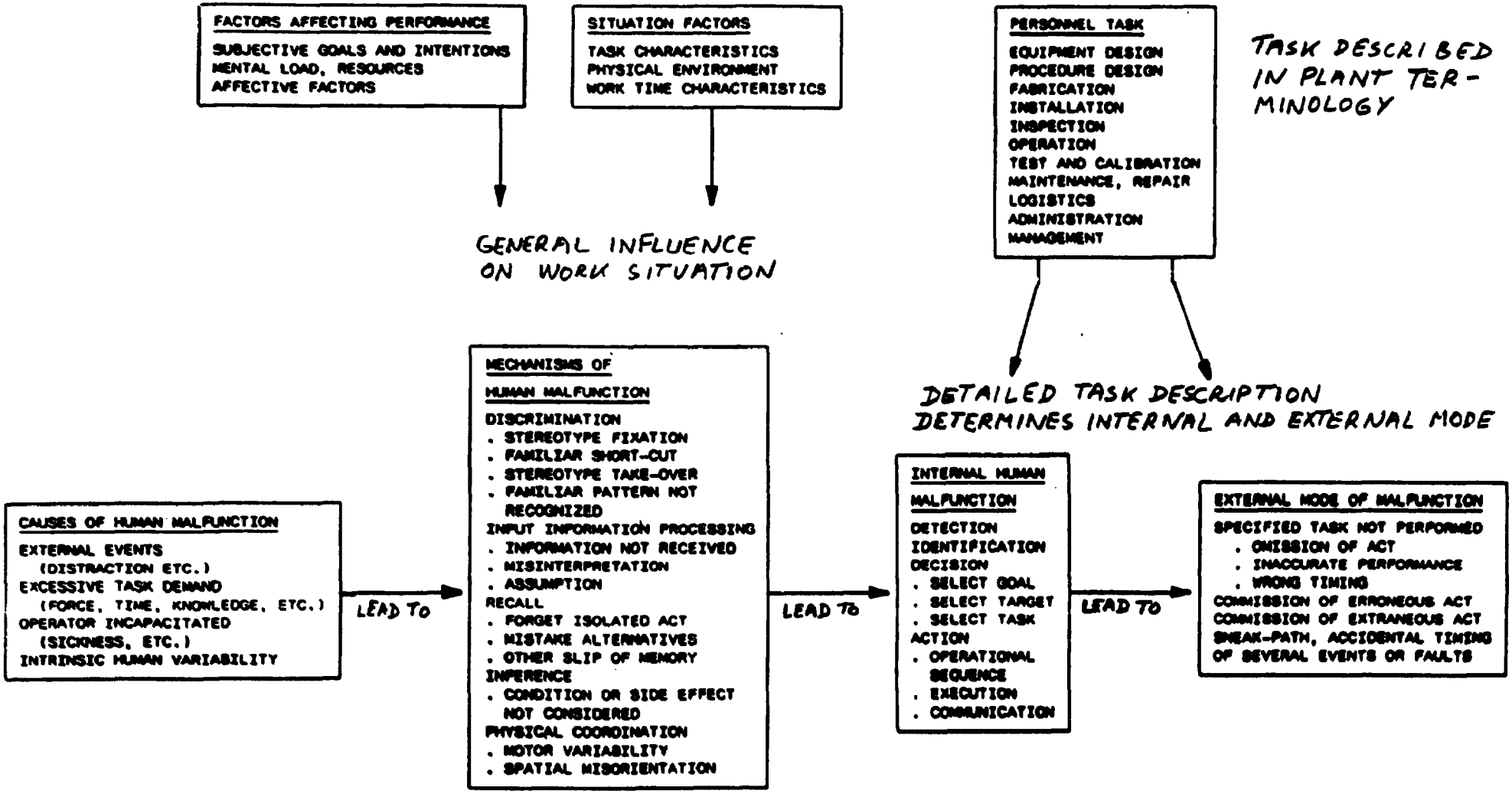


Figure A.1: Description system for human malfunctions

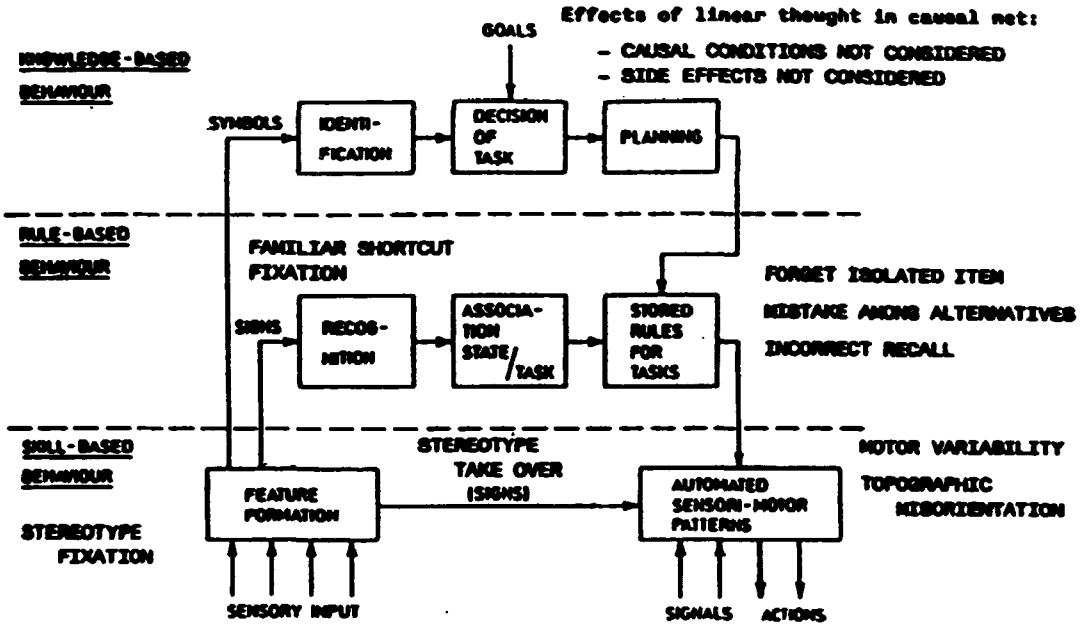


Figure A.2: Simplified map of three levels of control of human actions. The three levels are in a real situation interacting in a much more complex way than shown. Also in the map are indicated typical psychological error mechanisms.

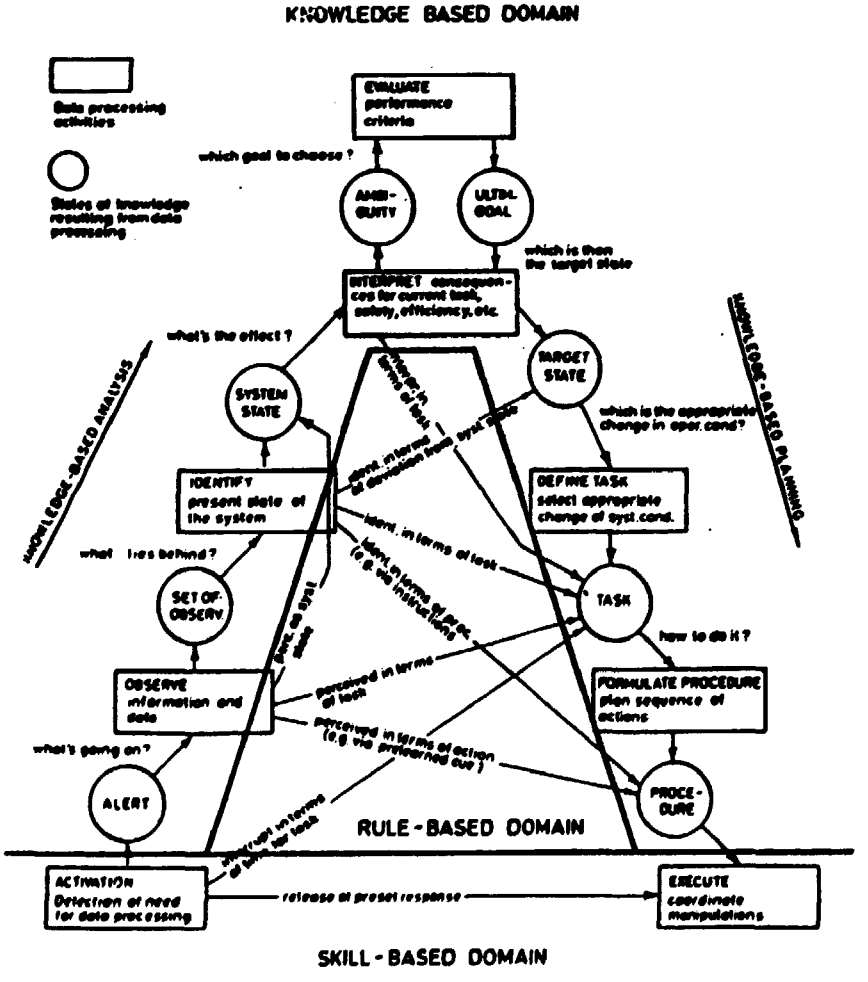


Figure A.3: Illustrates the relationship between the decision ladder and the three levels of control of human behaviour.

REFERENCES

(1) J. Rasmussen and O. M. Pedersen, Formalized Search Strategies for Human Risk Contributions: A Framework for Further Development. NKA/LIT-1(82)101. Also in Risø-M-2351, 1982.

(2) J. Rasmussen, What Can Be Learned from Human Error Reports. In: Duncan, K., Gruneberg, M., and Wallis, D. (Eds).: Changes in Working Life, John Wiley & Sons (Proceedings of the NATO International Conference on Changes in the Nature and Quality of Working Life, Thessaloniki, Greece, 1980).

(3) J. Rasmussen et al., Classification System for Reporting Events Involving Human Malfunction, Risø-M-2240, 1981.

(4) J. Rasmussen, Notes on Human Error Analysis and Prediction. In: Synthesis and Analysis Methods for Safety and Reliability Studies, Apostolakis, G., and Volta, G. (Eds), Plenum Press, London, 1980.

INDEX

Risø National Laboratory

Risø-M- 2513

Risø-M- 2513

Title and author(s)

Human Risk Contributions in Process Industry: Guides for Their Pre-Identification in Well-Structured Activities and for Post-Incident Analysis.

O. M. Pedersen

Date
May 1985

Department or group
Electronics

Group's own registration number(s)
R-3-85
NKA/LIT-1(84)106

pages + tables + illustrations

Abstract

The report should be considered a guide for the treating of human errors: for identifying their possibilities of occurrence when designing well-structured human tasks and for their improvement when they occur in reality.
For these purposes a strong coupling between predictive and retrospective analysis is emphasized: In order to control human errors, post-incident analysis of cases with human errors in a given industrial plant should be performed as means of feedback from reality for the verification of results of predictive analysis and also as a general means of identifying and improving such human errors which cannot be expected covered by predictive analysis.

Primarily, the guide addresses people with a knowledge of the technical plant in question and involved in the safety-oriented design and improvement of human activities and without a particular human factors background.

The main report describes the procedures for post-incident analysis and for Work Analysis, which is a search strategy developed for well-defined activities, e.g. test and calibration, and constitutes a formalized procedure for the pre-identification of relevant human errors leading to a lack of task result and/or to immediate effects not covered by the lack of task result itself.

Work Analysis and the post-incident analysis procedure are based on a common description system for human malfunctions. This system is explained in appendix and so are its underlying models and way of reasoning.

Finally, a word index is provided for supporting the reader.

4 references. In English.

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø),
DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116

Copies to

Available on request from.
Risø Library,
Risø National Laboratory, P.O. Box 49,
DK-4000 Roskilde, Denmark
Phone (02) 37 12 12 ext.2262

ISBN 87-550-1124-1
ISBN 0418-6435